THALES

Thales Luna K7 Cryptographic Module

NON-PROPRIETARY SECURITY POLICY

Used as a Standalone Device as ‘Thales Luna PCIe HSM’ OR as an Embedded Device in ‘Thales Luna Network HSM’

FIPS 140-2, Level 3

Document Information

Document Part Number	002-010935-002
Release Date	March 8, 2023

Revision History

Revision	Date	Reason
A	June 18, 2020	Updated SP for FW release 7.7.0. The document has been updated to be consistent in style other Thales SP including updates to both branding and product name. The document builds on 002-010935-001.
B	July 21, 2020	Updated Vendor Affirmation claims to be consistent with FIPS IG G.13.
C	July 29, 2020	Simplified services table listings.
D	November 2, 2020	Updated for FW 7.7.1 as well as minor fixes.
E	December 16, 2020	Updated to address Coordination comments and to add algorithm certs for KAS-FFC-SSC SP 800-56Ar3, KAS-ECC-SSC SP 800-56Ar3 and KAS-KDF OneStep SP 800-56Cr1.
F	January 8, 2021	Corrected typographic error in KDA cert number in Table 8. Corrected incorrectly mapped certificate number to KAS-SSC in Table 8.
G	March 5, 2021	Updated Table 8 to comply with requirements in IG A.11 for use of SHA-3 with higher-order algorithms without available CAVP testing. Updated Table 8 and Table 9 to comply with requirements from IG D.4, G.13, D.8 and D.9 in relation to KTS, KAS, SP 800-56B and allowances for RSA key transport. Updated references to SP 800-56Br2 to SP 800-56B throughout.
H	May 5, 2021	Updated Table 8 to add algorithm certificates, replacing vendor affirmations.
J	June 17, 2021	Updated references to SP 800-56B to SP 800-56Br2 throughout. Added missing CKG Vendor Affirmation to Table 8.

		Corrected entry from SP 800-56Br2 KAS1-Basic in Table 8 to be consistent with IG G.13. Expanded footnote 7 to make is clear duplicated KAS listings under Cert #A480 are required and intended. Added footnote 10 against PBKDF entry in Table 8 to provide further details on the limitations on use of algorithm by the module. Added further guidance and information on use of PBKDF to section 2.4.1.
K	October 25, 2021	Minor updates to key strength claims X9.42 CVL text modification
L	March 18, 2022	Added two part hardware versions to reflect minor parts supply issue.
M	April 18, 2022	Corrected hardware part number typos
N	December 9, 2022	Added bootloader 1.1.5 and firmware 7.7.1-20 to address bug fixes
P	March 8, 2023	Corrected typo

Trademarks, Copyrights, and Third-Party Software

Disclaimer

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

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

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media other than on the NIST CMVP validation list 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 makes no warranty as to the value or accuracy of information contained herein.

Thales 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 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 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 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 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

ACRONYMS AND ABBREVIATIONS

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AU	AUdit
API	Application Programming Interface
CBC	Cipher Block Chaining
CID	Client IDentity
CITS	Chrysalis ITS
CFB	Cipher FeedBack
CMAC	Cipher-based Message Authenticate Code
CO	Crypto Officer
CPV1	Cloning Protocol Version 1
CPV3	Cloning Protocol Version 3
CSK	CSP Wrapping Key
CSP	Critical Security Parameter
CTR	CounTeR
CU	Crypto User
CVL	Component Validation List
DAK	Device Authentication Key
DAC	Device Authentication Certificate
DEK	Data Encryption Key
DH	Diffie Hellman
DMK	Data MAC Key
DPK	Data Protection Key

Term	Definition
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
EFP	Environmental Failure Protection
EKA	Ephemeral Key Agreement
EMC	ElectroMagnetic Compliance
EMI	ElectroMagnetic Interference
FIPS	Federal Information Processing Standard
FM	Functional Module
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
GSK	Global Storage Key
HMAC	Keyed-Hash Message Authentication Code
HA	High Availability
HOC	Hardware Origin Certificate
HOK	Hardware Origin Key
HSE-BBRAM	High-speed erase battery backed RAM
HSM	Hardware Security Module / Host Security Module
ICD	Interface Control Design/Document
IG	Implementation Guidance
I/O	Input/Output
IV	Initialization Vector
KAT	Known Answer Test
KBKDF	Key-Based Key Derivation Function
KCV	Key Cloning Vector

Term	Definition
KDF	Key Derivation Function
KEK	Key Encryption Key
KEV	Key Encryption Vector
KTS	Key Transport Scheme
KW	Key Wrap mode
KWP	Key Wrap with Padding mode
LCO	Limited Crypto Officer
LED	Light Emitting Diode
MAC	Message Authentication Code
Masking	A Thales term to describe the encryption of a key for use only within a Thales cryptographic module.
MGF	Mask Generation Function
MIC	Manufacturer's Integrity Certificate
MIK	Manufacturer's Integrity Key
MK	Master Key
N/A	Not Applicable
OFB	Output FeedBack
PBKDF	Password-based Key Derivation Function
PSK	Partition Storage Key
PCI-E	Peripheral Component Interconnect
PEC	Password Encryption Certificate
PED	PIN Entry Device
PEK	Password Encryption Key
PKCS	Public-Key Cryptography Standards
POST	Power-on Self-Test
RDK	Role Domain Key
RNG	Random Number Generator

Term	Definition
RPK	Remote PED Key
RPV	Remote PED Vector
RSA	Rivest Shamir Adleman
RTC	Real Time Clock
SALK	Secure Audit Logging Key
SHA	Secure Hash Algorithm
SKA	Static Key Agreement
SMK	SKS Master Key
SKS	Scalable Key Storage
SMK	Security Officer’s Master Key
SO	Security Officer
SP	Special Publication
STC	Secure Trusted Channel
STM	Secure Transport Mode
TDES	Triple – Data Encryption Standard
TUK	Token or Module Unwrapping Key
TVK	Token or Module Variable Key
TWC	Token or Module Wrapping Certificate
USB	Universal Serial Bus
USK	User’s Storage Key
VPD	Vital Product Data
XEX	XOR-encrypt-XOR
XOR	eXclusive OR
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing

PREFACE

This document deals only with operations and capabilities of the Thales Luna K7 Cryptographic Module in the technical terms of FIPS PUB 140-2, 'Security Requirements for Cryptographic Modules', 12-03-2002.

General information on Thales HSM alongside other Thales products is available from the following sources:

> the Thales internet site contains information on the full line of available products at https://cpl.thalesgroup.com

> product manuals and technical support literature is available from the Thales Customer Support Portal at https://supportportal.thalesgroup.com/csm

> technical or sales representatives of Thales can be contacted through one of the channels listed on https://cpl.thalesgroup.com/contact-us

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.

1 Introduction

1.1 Purpose

This document describes the security policies enforced by the Thales Luna K7 Cryptographic Module.

1.2 Scope

This document applies to hardware part numbers 808-000048-002, 808-000048-003, 808-000066-001, 808-000073-001 and 808-000073-002 with firmware version 7.7.0, 7.7.1, or 7.7.1-20, with bootloader version 1.1.1, 1.1.2, 1.1.4, and 1.1.5 and where:

- 808-000048-002 and 808-000048-003 correspond to a module with fans on the outside of the metal enclosure factory installed;
- 808-000073-001 and 808-000073-002 correspond to a module with extra heatsinks installed (instead of fans as pictured);
- 808-000048-002 and 808-000048-003 are functionally equivalent with the difference being limited to the supply choice for one of the non-security enforcing internal components;
- 808-000073-001 and 808-000073-002 are functionally equivalent with the difference being limited to the supply choice for one of the non-security enforcing internal components; and
- 808-000066-001 and 808-000073-001 are alternate part numbers for the same hardware with no functional changes.

The security features described in this document apply to the Thales Luna K7 Cryptographic Module only and do not include any feature that may be enforced by the host appliance, client or Thales Luna PED.

The Thales Luna K7 Cryptographic Module can be used as follows:

- as a standalone device called the Thales Luna PCIe HSM; or
- as an embedded device in the Thales Luna Network HSM.

This document covers both the PED and Password Authentication (FIPS Level 3**)** configurations of the Thales Luna K7 Cryptographic Module.

1.3 Validation Overview

The cryptographic module meets all level 3 requirements security requirements for FIPS 140-2, alongside the optional Environment Failure Protection (EFP) augmentation as summarized in the table below:

Table 1: FIPS 140-2 Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	3

Security Requirements Section	Level
Cryptographic Module Ports and Interfaces	3
Roles and Services and Authentication	3
Finite State Machine Model	3
Physical Security	3 + EFP
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3
Cryptographic Module Security Policy	3

1.4 Functional Overview

The Thales Luna K7 Cryptographic Module is a multi-chip embedded hardware cryptographic module in the form of a PCI-Express card that typically resides within a custom computing or secure communications appliance. The cryptographic module is contained in its own secure enclosure that provides physical resistance to tampering.

The cryptographic boundary of the module is defined to encompass all components inside the secure enclosure on the PCI-E card.

A module may be explicitly configured to operate in either FIPS 140-2 Approved mode, or in a non-FIPS mode of operation using steps outlines in section 3 and where these are performed during initialization of the module.

The module only supports a single approved mode of operation as set out in FIPS IG 1.7 ‘Multiple Approved Modes of Operation’ and any configuration changes to settings defining the ‘Approved Mode of Operation’ will trigger a zeroization of all partition CSP and require the full reset and re-initialization of the module.

A module is accessed directly (i.e., electrically) over the PCI-Express communications interface. If configured the Thales Luna PIN Entry Device (PED) can be connected to the module’s USB port for authentication.

A module provides secure key generation and storage for symmetric keys and asymmetric key pairs along with support for a broad range of cryptographic services. Access to key material and cryptographic services for users and user application software is provided through the PKCS #11 programming API, which is implemented over the module’s proprietary command interface (ICD).

A module may host multiple ‘user partitions’ that are cryptographically separated and are presented as “virtual tokens” to user applications. A single ‘admin partition’ exists that is dedication to the HSM Security Officer and Administrator roles. Each partition must be separately authenticated in order to make it available for use.

2 Module Overview

2.1 Module Specification

The cryptographic module is a multi-chip embedded hardware module which is available by itself as the Thales Luna PCIe HSM or embedded within the Thales Luna Network HSM.

The cryptographic boundary[1] of the module is shown below. The cryptographic boundary is defined as the metal enclosure on the top and bottom sides of the PCI-E card as outlined. The fans depicted alongside the removable backup battery are not included in the cryptographic boundary.

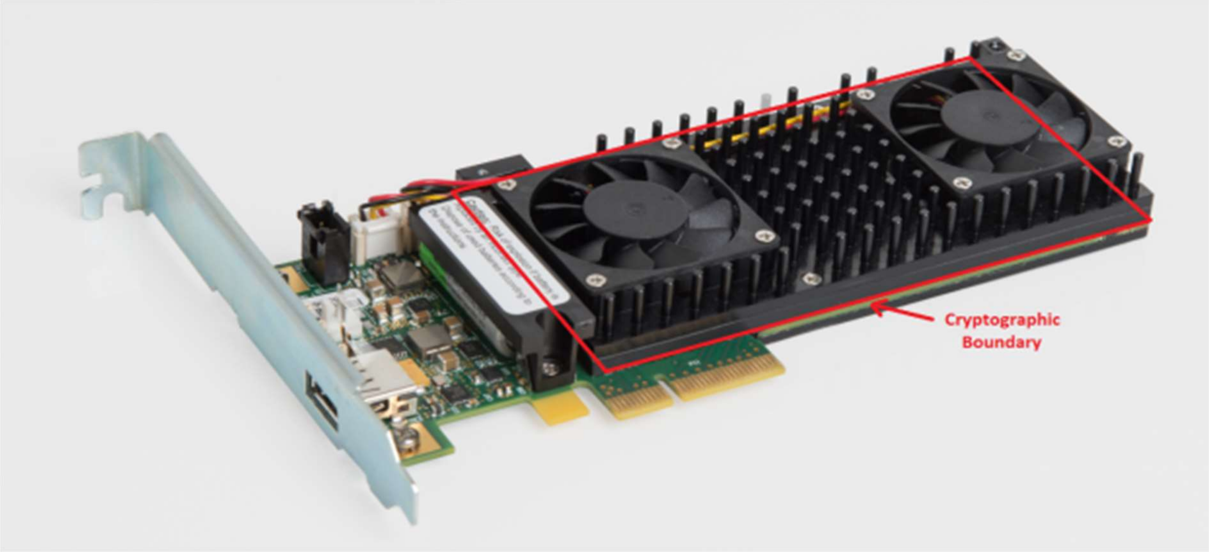

Figure 1: Thales Luna K7 Cryptographic Module cryptographic boundary

Figure 2: Thales Luna Network HSM

[1] The fans depicted are not included in the physical boundary of the module. The 808-000066-001, 808-000073-001 and 808-000073-002 variants of the module do not include fans.

2.2 Ports and Interfaces

2.2.1 Ports and Interface Overview

The module supports the following physical ports and interfaces:

> PCI-E interface

> USB port

> Serial port

> Power supply

> Battery

> LED

> External event input

> Decommission input

Table 2: Mapping of FIPS 140-2 Interfaces to Physical and Logical Interfaces

FIPS 140-2 Interface	Physical Interface	Logical Interface
Data Input	PCI-E interface	Data I/O Luna ICD Logical Trusted Path (Luna PED - remote connection) Bootloader command protocol
	USB	Physical Trusted Path (Luna PED - local connection)
	Serial interface	Bootloader command protocol
Data Output	PCI-E interface	Data I/O Luna ICD Logical Trusted Path (Luna PED – remote connection) Bootloader command protocol
	USB	Physical Trusted Path (Luna PED – local connection)
	Serial Port	Bootloader command protocol
Control Input	PCI-E interface	Data I/O Luna ICD
	External event jumper	N/A
	Decommission jumper	N/A

FIPS 140-2 Interface	Physical Interface	Logical Interface
	Serial Port	Luna Communication Path
Status Output	PCI-E interface	Data I/O Luna ICD Logical Trusted Path (Luna PED - remote connection) Bootloader command protocol
	USB	Physical Trusted Path (Luna PED - local connection)
	LED	N/A
	Serial Port	Bootloader command protocol
Power	5V and 1.8V (generated from 12V power supply via PCI-E interface)	N/A
	3.6V battery	N/A

2.2.2 Luna PED (local connection)

If configured, the module can use a Luna PED as an external data input/output device. The Luna PED connects to the module's USB port and is used to pass authentication data and CSPs to and from the module via a physical trusted path. CSP's and authentication data that are output to the Luna PED are stored in a PED Key (also known as an iKey) USB device connected to the Luna PED.

Any PED Key, once data has been written to it, is an Identification and Authentication device and must be safeguarded accordingly by the administrative or operations staff responsible for the operation of the module within the customer's environment.

The following types of PED Keys[2] are used with the Luna PED:

> Orange (RPV) PED Key – for the storage of the Remote PED Vector (RPV);

> Blue (Security Officer) PED Key – for the storage of HSM Security Officer, Partition Security Officer and Administrator authentication data[3];

> Black (Crypto Officer) PED Key – for the storage of Crypto Officer (or Limited Crypto Officer (LCO)) authentication data;

> Grey (Crypto User) PED Key – for the storage of Crypto User authentication data;

> Red (Cloning Domain) PED Key – for the storage of the cloning domain data, used to control the ability to clone to another cryptographic module or to a backup module; and

[2] Separate PED Keys are used when M of N token splitting is used to share responsibilities for this role between different operators.

[3] Separate PED Keys can be used when these roles are assigned to different operators

- White (Audit) PED Key – for the storage of Audit user authentication data.

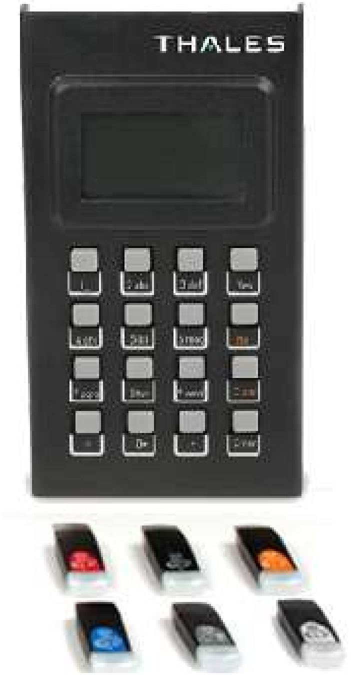

Figure 3: Thales Luna PIN Entry Device (PED) and iKey

2.2.3 Luna PED (remote connection)

If configured, the user has the option of operating the Luna PED remotely, connected to a USB port on a management workstation. Remote PED operation extends the physical trusted path connection by the use of a secure protocol over the PCI-E interface that authenticates both the remote PED and the module and establishes an encrypted and authenticated communications channel between the module and the Remote PED. Once secure communications have been established, all interactions between the cryptographic module, PED, and PED Keys are performed in exactly the same way as they would be when locally connected.

The logical path between the cryptographic module and the Remote PED is secured in the manner described below:

- Luna PED and cryptographic module will use the C(2e, 2s, ECC CDH) scheme from NIST SP 800-56Ar3 to establish a CSP Wrapping Key (CWK) and MAC key (DMK) for encrypting the session and authenticating each other.
- Encryption of messages between the Luna PED and cryptographic module uses AES-256 in CTR Mode and with each encrypted message additionally protected using a HMAC-256 MAC.

Sensitive data in transition between a Luna PED and an HSM is end-to-end encrypted: plaintext PED data is never exposed beyond the HSM and the Luna PED boundaries at any time. Inherent security of the PED/HSM connection and associated protocols allows the usage of otherwise unprotected communications all the way through the data path between the devices.

2.2.4 Secure Messaging

Each partition can optionally be configured to use a secure messaging feature called Secure Trusted Channel (STC). An STC channel is a cryptographic tunnel established between a partition and the Thales Luna Client running on a host which may either be:

- local to the Thales Luna K7 Cryptographic Module; or
- running on a remote host.

The STC channel is designed to provide confidentiality, authenticity and integrity on all ICD commands that are sent to the partition.

Clients are pre-registered with a target partition requiring STC using a supplied public key used to authenticate them and where the Cryptographic Module is separately pre-registered at the client based on a supplied certificate registered at the client.

The STC protocol uses C(2e, 2s, ECC CDH) scheme from NIST SP 800-56Ar3 to establish shared encryption and optionally message authentication keys. Following the key exchange the transport protocol can be configure to use one of two cipher suites for message transmission:

- AES-256 using GCM as an authenticated encryption mode; or
- AES-256 using CTR mode alongside HMAC-SHA512,

for its encryption and authentication.

2.3 Roles and Services

2.3.1 Roles

The Thales Luna K7 Cryptographic Module supports the following roles:

Table 3: Thales Luna K7 Cryptographic Module Roles

Roles	Principal Duties
HSM Security Officer (HSM SO) [Admin Partition Role]	The HSM SO is responsible for managing the HSM. As such, he/she is authorized to install and configure the HSM, set and maintain global HSM security policies. He/she is also able to request the load of new HSM firmware update files (FUF) and new Configuration Update Files (CUF). 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.
Administrator [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.

Roles	Principal Duties
Partition Security Officer (Partition SO) [User Partition Role]	The Partition SO creates the partition level Partition CO role, sets and changes partition-level policies. This role also has an option to reset the Partition CO password (configuration dependent) following lockout.
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 [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.

The mapping of the cryptographic module's roles to the roles defined in FIPS 140-2 can be found in the table below:

Table 4: Mapping of FIPS 140-2 Roles to Module Roles

FIPS 140-2 Role	Thales Luna K7 Cryptographic Module Role	Role Scope
Crypto Officer	HSM Security Officer (HSM SO)	Module
	Audit	Module
	Partition Security Officer (Partition SO)	User Partition
User	Administrator	Admin Partition
	Crypto Officer	User Partition
	Partition Crypto Officer (Partition CO)	User Partition
	Partition Limited Crypto Officer (Partition LCO)	User Partition
	Partition Crypto User (Partition CU)	User Partition

FIPS 140-2 Role	Thales Luna K7 Cryptographic Module Role	Role Scope
Unauthenticated User	Public User	Module/Partition

2.3.2 Services

All services listed in the table below can be accessed in FIPS 140-2 Approved mode and when in this mode exclusively use the security functions listed in Table 8 and Table 9.

When the module is operating in this mode, Security Functions in section 2.7.2 are disabled and blocked from being used.

For a complete description of CSP referenced from the table please see Table 10.

Table 5: Roles and Access Rights by Service

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
HSM Management										
HSM Factory Reset.	**Erased (for ALL partition):** PSK, USK, DRBG Key, DRBG Seed, DRBG V, KCV, SMK, STC-PID$_{PUB}$, STC-PID$_{PRIV}$, STC-CID$_{PUB}$, STC-PID$_{PUB}$, STC-PKA$_{PUB}$, STC-PKA$_{PRIV}$, STC-CKA$_{PUB}$, STC-PEN, STC-PMA, STC-PIV, STC-CEN, STC-CMA, STC-CIV. HA$_{PUB}$, HA$_{PK}$, RND, Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys). In addition, the following HSM level keys are erased: DRBG Key, SALK, CWK$_{HSM}$, CWK$_{PED}$, DEK$_{HSM}$, DMK$_{HSM}$, DEK$_{PED}$, DMK$_{PED}$.	x	x	x	x	x	x	x	x	Does not require user login. Factory reset deletes all roles (including HSM SO), all users and objects and sets all HSM settings and policies to default values. Can be performed by any role as equivalent to destroying the HSM through other means if physical access to the HSM is possible. Only possible over the serial connection to LUSH when Luna PCI-E K7 is embedded in Thales Luna Network HSM.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Initialize the HSM (operation resets the admin partition, deletes all user partitions (if present), initializes the HSM SO role and creates / selects cloning domain secret (KCV)).	**Erased:** For ALL partition if present **–** USK, PSK, SMK, Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys). For User Partitions: HA_{PUB}, HA_{PK} (for all roles). For Admin Partition - HA_{PUB}, HA_{PK} for Admin role only. **Write:** PEK, PEC, USK, PSK, DRBG Key, DRBG Seed, DRBG V, KCV. **Used:** PSK, USK, GSK.	x	x	x	x	x	x	x	x	Operation must be performed by the HSM SO unless the HSM has been factory reset first. If performed without the factory reset, the HSM SO, AU and KCV for the Admin Partition are maintained through initialisation. If factory reset has been performed prior to initialising the HSM SO, any role with the ability to access the LunaCM (Thales Luna PCIe HSM) or LunaSH (Thales Luna Network HSM) Command Line Interface (CLI) can perform initialization. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Create a user partition.	**Write:** DRBG Key, DRBG Seed, DRBG V, KCV.	x	-	-	-	-	-	-	-	None.
Delete a user partition.	**Erased (for partition instance of key object):** PSK, USK, DRBG Key, DRBG Seed, DRBG V, KCV, SMK, STC-PID_{PUB}, STC-PID_{PRIV}, STC-CID_{PUB}, Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys).	x	-	-	-	-	-	-	-	Deleting a partition erases all partition object and roles.
Query HSM status.	None.	x	x	x	x	x	x	x	x	This service is permitted from an un-authenticated client even if STC is enabled.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Query partition status.	None.	x	x	x	x	x	x	x	x	This service is permitted from an un-authenticated client even if STC is enabled.
Query HSM configuration.	None.	x	x	x	x	x	x	x	x	None.
Query partition configuration.	None.	x	x	x	x	x	x	x	x	None.
Set HSM Level Policy (General).	**Erased (if destructive policy change requested):** For all partitions: Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys), USK, PSK, KCV, SMK, STC-PID$_{PRIV}$, STC-PID$_{PUB}$. The following are erased in addition if HSM Policy (50) 'Allow Functional Modules' is enabled: HOK, HOC, ECC HOK, ECC HOC,TUK4,TWC4, CITS-DAK, CITS-DAC, ECC DAK, ECC DAC, HSM-SKA-C$_{REMOTE}$, HSM-SKA-K$_{LOCAL}$, PAC, RPV-C, PEK, PEC.	x	-	-	-	-	-	-	-	None.
Set Partition Level Policy (Admin Partition).	**Erased (if destructive policy change requested):** Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys), SMK.	x	-	-	-	-	-	-	-	None.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Set Partition Level Policy (User Partition).	**Erased (if destructive policy change requested):** Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys), SMK.	-	-	-	x	-	-	-	-	None.
Update Firmware.	**Used:** Root Certificate, Firmware Signing Certificate**.**	x	-	-	-	-	-	-	-	None.
Trigger HSM zeroization / decommission.	**Erase:** As per Factory Reset above but with the following omissions: CSP associated with the Audit partition and AU role are not zeroized and persist. RPV persists.	x	x	x	x	x	x	x	x	Can be performed by any role. Equivalent to destroying the HSM through other means if physical access to the HSM is possible. Only possible over the serial connection to LUSH when Thales Luna K7(+) Cryptographic Module is embedded in Thales Luna Network(+) HSM.
Trigger user partition zeroize.	**Erased:** USK, PSK,KCV, SMK, Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys).	x	x	x	x	x	x	x	x	This command is currently supported by the Luna ICD command library but isn't currently made available using any of the customer facing API (such as the Cryptoki API).
Load Configuration Update File (CUF).	**Used:** Root Certificate and License Signing Certificate.	x	-	-	-	-	-	-	-	None.
Query the audit log status.	None.	x	x	x	x	x	x	x	x	None.
Submit external messages for entry into secure audit log.	**Used:** SALK.	x	x	x	x	x	x	x	x	None.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Configure the audit logging level and destination for offload.	None.	-	-	x	-	-	-	-	-	None.
Export/import audit log secret key.	**Used:** RDK **Read:** SALK	-	-	x	-	-	-	-	-	None.
Set time on HSM Real Time Clock (RTC).	None.	-	-	x	-	-	-	-	-	The RTC is used for time-stamps on logs and separately for enforcing `CKA_START_DATE` and `CKA_END_DATE` object attributes when **Partition Policy (39) Allow Start/End Date Attributes** is enabled.
Validate the audit log.	**Used:** SALK.	-	-	x	-	-	-	-	-	None.
Request Partition STC Identity.	**Use:** STC-PID$_{PUB}$ **Write:** STC-PID$_{PRIV,}$ STC-PID$_{PUB}$	x	x	x	x	x	x	x	x	STC-PID$_{PRIV,}$ STC-PID$_{PUB}$ are created on first attempted read of the public certificate.
Register/De-register client for STC (admin partition).	**Write:** STC-CID$_{PUB}$	x	-	-	-	-	-	-	-	None.
Register/De-register client for STC (user partition).	**Write:** STC-CID$_{PUB}$	x	-	-	x	-	-	-	-	None.
Query registered STC client status information (admin partition).	None.	x	-	-	-	-	-	-	-	None.
Query registered STC client status information (user partition).	None.	-	-	-	x	-	-	-	-	None.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Initiate STC Tunnel once configured.	**Use:** STC-PID$_{PRIV}$, STC-CID$_{PUB}$, ECC HOC, GSK. **Create:** STC-PKA$_{PUB}$, STC-PKA$_{PRIV}$**,** STC-PEN, STC-PMA, STC-PIV, STC-CEN, STC-CMA, STC-CIV.	x	x	x	x	x	x	x	x	None.
Send commands to partition with STC tunnel initiated.	**Use:** STC-PEN, STC-PMA, STC-PIV, STC-CEN, STC-CMA, STC-CIV.	x	x	x	x	x	x	x	x	This service includes the dispatch and receipt of commands and responses to a target partition with an active STC tunnel. Privileges involve the ability to dispatch messages only and authentication of any active session as another role is required over-STC ahead of performing any privileged operation.
Clone SMK between Partitions.	**Use:** Root Certificate, MIC, HOC (or FM equivalent) and TUK4, TWK4, KEV$_s$ (CPV1 only), KEV$_t$, KCV and Cloning Transfer Key. **Read/Write**: SMK.	x	-	-	-	x	-	-	-	HSM SO is able to clone (or receive) the SMK from/to the Admin Partition. Partition CO is able to clone (or receive) the SMK from/to the user partition.
Clone partition objects between Partitions.	**Use:** Root Certificate, MIC, HOC (or FM equivalent) and TUK4, TWK4, KEV$_s$ (CPV1 only), KEV$_t$, KCV and Cloning Transfer Key.	x	x	-	-	x	x	x	-	Partition CU is able to clone public key objects only.
Rollover SMK for a given partition.	**Use:** USK, DRBG Key, DRBG Seed, DRBG V. **Write:** SMK, DRBG Key, DRBG Seed, DRBG V.	x	-	-	-	x	-	-	-	HSM SO can trigger roll-over of the SMK on the admin partition. Partition CO can trigger roll-over of the SMK on the user partition.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Enable/disable STM.	**Create:** STM Nonce. **Use:** STM Nonce, DRBG Key, DRBG Seed, DRBG V (DRBG only used to create STM None on enabling STM).	x	x	x	x	x	x	x	x	Command can be executed un-authenticated if HSM is in zeroized state otherwise requires HSM SO role.
Clear tamper event.	None.	x	x	x	x	x	x	x	x	Only required when HSM **Policy (48): Do Controlled Tamper Recovery** is enabled. Command can be executed un-authenticated if HSM is in zeroized state otherwise requires 'HSM SO'.
Request HSM self-test operation.	None.	x	x	x	x	x	x	x	x	None.
Role Management										
Query Role Status.	None.	x	x	x	x	x	x	x	x	None.
Initialize the Administrator.	**Use:** DRBG Key, DRBG Seed, DRBG V, USK, PSK, KEK, PEK. **Write:** PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password.	x	-	-	-	-	-	-	-	PEK is only used if the authentication date is submitted over Luna ICD command. PEK and PEC are only created if not already present on the cryptographic module. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Initialize the AU.	**Use:** DRBG Key, DRBG Seed, DRBG V, USK, PSK, KEK, PEK. **Write:** PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password.	x	x	x	x	x	x	x	x	AU can be initialized from a public session to the Admin partition of the HSM, hence is accessible to all roles. In Thales Luna Network HSM, the role is initialized by the Audit user appliance role. PEK is only used if the authentication date is submitted over Luna ICD command. PEK and PEC are only created if not already present on the cryptographic module. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Initialize the Partition SO.	**Use:** DRBG Key, DRBG Seed, DRBG V, KEK, PEK. **Write:** USK, PSK, PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password.	x	x	x	x	x	x	x	x	PEK is only used if the authentication data is submitted over Luna ICD command. PEK and PEC are only created if not already present on the cryptographic module. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Initialize the Partition CO.	**Use:** DRBG Key, DRBG Seed, DRBG V, USK, PSK, KEK, PEK. **Write:** PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password.	-	-	-	x	-	-	-	-	PEK is only used if the authentication date is submitted over Luna ICD command. PEK and PEC are only created if not already present on the cryptographic module. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Initialize the Partition LCO.	**Use:** DRBG Key, DRBG Seed, DRBG V, USK, PSK, KEK, PEK. **Write:** PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password.	-	-	-	-	x	-	-	-	PEK is only used if the authentication date is submitted over Luna ICD command. PEK and PEC are only created if not already present on the cryptographic module. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Initialize the Partition CU.	**Use:** DRBG Key, DRBG Seed, DRBG V, USK, PSK, KEK, PEK. **Write:** PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password.	-	-	-	-	x	-	-	-	PEK is only used if the authentication date is submitted over Luna ICD command. PEK and PEC are only created if not already present on the cryptographic module. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Change HSM SO authentication data.	**Read:** USK **Use:** KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** USK.	x	-	-	-	-	-	-	-	Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Change AU authentication data.	**Read:** USK **Use:** USK, KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** USK.	-	-	x	-	-	-	-	-	Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Change authentication data for Administrator / unlock role.	**Read:** USK **Use:** KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** USK.	x	x	-	-	-	-	-	-	Only possible for HSM SO if **HSM Policy (15) Enable SO reset of partition PIN** is enabled. If the service is performed by the HSM SO, this is considered as unlock operation after Administrator role is locked out. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Change Partition SO authentication data.	**Read:** USK **Use:** KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** USK.	-	-	-	x	-	-	-	-	Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Change authentication data for Partition CO / unlock role.	**Read:** USK **Use:** KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** USK.	-	-	-	x	-	-	-	-	Only possible if **HSM Policy (15) Enable SO reset of partition PIN** is enabled. Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Change authentication data for Partition LCO / unlock role.	**Read:** USK **Use:** KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** USK.	-	-	-	-	x	x	-	-	If the service is performed by the Partition CO, this is considered as an unlock operation after the Partition LCO role is locked out.
Change authentication data for Partition CU / unlock role.	**Read:** USK **Use:** KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** USK.	-	-	-	-	x	-	x	-	If the service is performed by the Partition CO, this is considered as an unlock operation after the Partition CU role is locked out.
Configure partition for High-Available (HA) Recovery / Login	**Use:** DRBG Key, DRBG Seed, DRBG V. **Write:** HA_{PUB}, HA_{PK}, DRBG Key, DRBG Seed, DRBG V. **Create:** RND, K_{sess}.	x	x	x	x	x	x	x	-	This service allows partitions to be registered in a way with a primary partition in order to allow login to the secondary partition following activation of the primary partition. The service can only be used if **Partition Policy (21) Enable high availability recovery** is enabled. Required role depends on the role desired to be configured for HA Recovery.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Login to Access/Session as role.	**Use:** KEK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password. **Write:** recovered USK, PSK, KCV, GSK, SMK (if configured) (on successful presentation of correct login credentials).	x	x	x	x	x	x	x	-	Where Luna PED is used in its remote configuration, additional CSP are used and written and are recorded following this table.
Close authenticated sessions.	**Erase:** USK, PSK, KCV, GSK, SMK (if configured), Asymmetric Key Pairs (session keys), Symmetric Keys (session keys).	x	x	x	x	x	x	x	x	`CA_CloseApplicationID` or `CA_CloseApplicationIDForContainer` can be executed un-authenticated and can be used to close all sessions and/or access. USK, PSK, KCV, GSK, SMK only erased if no open sessions remain for a given Access.
Luna PED Configuration										
Initialize Remote PED Vector (RPV).	**Use:** GSK. **Write:** RPV.	x	-	-	-	-	-	-	-	None.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Key Management Activities										
Generate local symmetric or asymmetric key-pair.	**Use:** USK, DRBG Key, DRBG Seed, DRBG V. **Write:** Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys), DRBG Key, DRBG Seed, DRBG V.	x	x	-	-	x	x	-	-	HSM SO and Administrator can only create keys in the Admin Partition (or session owned by admin partition for session based keys). Partition CO and LCO can only create keys in their corresponding user partition (or session owned by user partition for session based keys).
Generate domain parameters.	**Use:** DRBG Key, DRBG Seed, DRBG V. **Write:** DRBG Key, DRBG Seed, DRBG V.	x	x	x	x	x	x	x	x	Domain parameter objects can be created by any role if `CKA_PRIVATE` key attribute is set to false. If `CKA_PRIVATE` is set to true – only HSM SO and Administrator can create in admin partition and Partition CO or LCO. As an output of the service a domain parameter object will be stored on the target partition which can be used as an input to subsequent key-pair generation operations.
Derive key from existing partition secret or private key object.	**Use:** Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys), USK, DRBG Key, DRBG Seed, DRBG V. **Write:** Symmetric Keys (general partition or session keys), DRBG Key, DRBG Seed, DRBG V.	x	x	-	-	x	x	-	-	`CKA_DERIVE` must be set to `true`. HSM SO and Administrator can only derive keys in the admin partition. Partition CO and Partition LCO in the user partition. Where PKA data is configured, both source and new PKA data must be provided during the operation. DRBG is only used where derive operations requires entropy (e.g. generation of random IV or randomised padding).

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Import public key, certificate, domain object or data objects.	**Write:** Asymmetric Key Pairs (general partition or session keys).	x	x	x	x	x	x	x	x	Listed objects can be created by any role if `CKA_PRIVATE` is set to `false`. If `CKA_PRIVATE` is set to `true` – only HSM SO and Administrator can create objects in the admin partition and Partition CO or LCO in the user partition.
Import secret or private key using key wrapping.	**Use:** Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys), USK. **Write:** Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys).	x	x	-	-	x	x	-	-	HSM SO and Administrator are only able to import to an admin partition. Partition CO and LCO are only able to import keys into the user partition they are a member of.
Export secret or private key using key wrapping.	**Read**: Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys). **Use**: Asymmetric Key Pairs (general partition or session keys), Symmetric Keys (general partition or session keys), DRBG Key, DRBG Seed, DRBG V, USK. **Write:** DRBG Key, DRBG Seed, DRBG V.	x	x	-	-	x	x	-	-	HSM SO and Administrator are only able to export keys from an admin partition. Partition CO and LCO are only able to export keys into the user partition they are a member of. DRBG is only used where encrypt operations require entropy (e.g. generation of random IV or randomised padding).
Read non-sensitive key attribute where `CKA_PRIVATE = false` for a given key object.	None.	x	x	x	x	x	x	x	x	None.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Read non-sensitive key attribute where `CKA_PRIVATE = true` for a given key object.	None.	x	x	-	-	x	x	x	x	None.
Insert key from external storage using SKS.	**Use:** SMK, USK. **Write:** Symmetric Keys (general partition or session keys) or Asymmetric Key Pairs (general partition or session keys)	x	x	-	-	x	x	x	-	HSM SO and Administrator are only able to insert keys for the admin partition. Partition CO, LCO and CU are only able to insert keys into the user partition they are a member of.
Extract key to external storage using SKS.	**Use:** SMK, USK. **Read:** Symmetric Keys (general partition or session keys) or Asymmetric Key Pairs (general partition or session keys)	x	x	-	-	x	x	x	-	HSM SO and Administrator are only able to extract keys from the admin partition. Partition CO, LCO and CU are only able to extract keys from the user partition they are a member of.
Explicitly revoke activation for key on a target session access.	None.	x	x	-	x	x	x	x	x	Explicit rescinding of activations can be performed using the `CA_AuthorizeKey` command with ‘0’ length authentication data supplied.
Cryptographic Services										
Re-seed partition random number generator (RNG).	**Use:** DRBG Key, DRBG Seed, DRBG V. **Write**: DRBG Key, DRBG Seed, DRBG V.	x	x	x	x	x	x	x	x	HSM SO, Administrator and AU are only able to seed the admin partition DRBG instance. Partition SO, CO, LCO and CU are only able to seed the user partition DRBG instance for the partition they are a member of. Key owner must separately be authenticated as another role listed.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Extract entropy from Partition DRBG.	**Use:** DRBG Key, DRBG Seed, DRBG V **Write** DRBG Key, DRBG Seed, DRBG V.	x	x	x	x	x	x	x	x	HSM SO, Administrator and AU are only able to extract entropy from the admin partition DRBG instance. Partition SO, CO, LCO are only able to extract entropy from the user partition DRBG instance they are a member of. Key owner must separately be authenticated as another role listed.
Perform digest operation on user supplied data.	None.	x	x	x	x	x	x	x	x	None.
Perform encrypt operation on user supplied data object.	**Use:** USK (if request requires access to key in non-volatile storage), Symmetric Keys (general partition or session keys), Asymmetric Key Pairs (general partition or session keys) – public key, DRBG Key, DRBG Seed, DRBG V. **Write:** DRBG Key, DRBG Seed, DRBG V.	x	x	x	x	x	x	x	x	Key owner must separately be authenticated as another role listed. DRBG is only used where encrypt operations requires entropy (e.g. generation of random IV or randomised padding). AU and PSO is only able to encrypt supplied data using public keys where `CKA_PRIVATE` for a given public key is `false`.
Perform decrypt operation on user supplied data object.	**Use**: USK (if request requires access to key in non-volatile storage), Symmetric Keys (general partition or session keys).	x	x	-	-	x	x	x	x	HSM SO and Administrator are only able to use keys stored in the admin partition. Partition CO, LCO and CU are only able to use keys in the user partition they are a member off. Key owner must separately be authenticated as another role listed.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Derive key	**Use:** USK (if request requires access to key in non-volatile storage), Symmetric Keys (general partition or session keys) or Asymmetric Key Pairs (general partition or session keys), DRBG Key, DRBG Seed, DRBG V. **Write:** Symmetric Keys (general partition or session keys), DRBG Key, DRBG Seed, DRBG V.	x	x	-	-	x	x	-	x	HSM SO and Administrator are only able to use keys stored in the admin partition. Partition CO, LCO are only able to use keys in the user partition they are a member off. Key owner must separately be authenticated as another role listed. DRBG is only used where derive operations require entropy.
Generate signature over user supplied data.	**Use:** USK (if request requires access to key in non-volatile storage), Symmetric Keys (general partition or session keys) or Asymmetric Key Pairs (general partition or session keys), DRBG Key, DRBG Seed, DRBG V. **Write:** Symmetric Keys (general partition or session keys), DRBG Key, DRBG Seed, DRBG V.	x	x	-	-	x	x	x	-	HSM SO and Administrator are only able to use keys stored in the admin partition. Partition CO, LCO, CU are only able to use keys in the user partition they are a member off. Key owner must separately be authenticated as another role listed. DRBG is only used where signature operations require entropy.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition LCO	Partition CU	Public User	Notes
Validate signature over user supplied data.	**Use:** USK (if request requires access to key in non-volatile storage), Symmetric Keys (general partition or session keys) or Asymmetric Key Pairs (general partition or session keys).	x	x	x	x	x	x	x	x	HSM SO and Administrator are only able to use keys stored in the admin partition. AU and PSO is only able to validate signatures with public keys where `CKA_PRIVATE` for a given public key is `false`. Partition CO, LCO, CU are only able to validate signatures in the user partition they are a member off. Key owner must separately be authenticated as another role listed.
Bootloader Services										
Set/Read scratchpad flag to signal to firmware	None.	x	x	x	x	x	x	x	x	Used exclusively to request un-authenticated deletion of the FM and/or SMFS to the firmware.
Request complete erase of the HSM firmware image and key stores (excludes erase of bootloader).	None.	x	x	x	x	x	x	x	x	Only used to recover from corrupt firmware as performed as a factory operation. Erases all CSP with the exception of the Root Certificate. Following erase, card needs to repeat manufacturing process including loading factory signed keys before it can be operational again.
Read Vital Product Data (VPD) programmed at Manufacture.	None.	x	x	x	x	x	x	x	x	Includes the hardware part number alongside whether PCIe card was built with fans or not installed.
Request authentication and execution of main firmware.	**Use:** Root Certificate and Firmware Signing Certificate.	x	x	x	x	x	x	x	x	None.

Where a service in Table 5 above involves the optional use of the Luna PED in its remote configuration, the following additional CSP are used or created by the target role using the Luna PED:

- **Used:** RPV, RPV-C, PAC, HSM-SKA-K_{LOCAL}, HSM-SKA-$K_{REMOTE,}$ PED-SKA-C.
- **Created:** $CWK_{HSM,}$ $CWK_{PED,}$ $DEK_{HSM,}$ $DMK_{HSM,}$ $IV_{HSM,}$ $DEK_{PED,}$ $DMK_{PED,}$ $IV_{PED.}$

2.4 Authentication

2.4.1 User Authentication

All roles except for the Public User must authenticate to the module by providing their authentication data. Table 6 and Table 7, explain the type and strength of the authentication data supported for each role.

If configured with PED, all roles must authenticate using a PED Key. When a role is initialized, a module generates the authentication data as a 48-byte random value and writes it to a PED Key. Optionally, the Crypto-Officer, Limited Crypto Officer and Crypto-User roles can be configured to use two-factor authentication by also assigning a password to the role.

If configured with Password, all roles must authenticate using a password. When a role is initialized under this configuration, the operator enters the initial password for the role.

Regardless of configuration (PED or Password), the password is delivered to the module encrypted with the module's Password Encryption Key (PEC) using KTS-OAEP: Key-Transport using RSA-OAEP from NIST SP 800-56Br2.

Table 6: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data	
		Password Configuration	**PED Configuration**
HSM Security Officer	Identity-based	Password	Authentication token (PED Key)
Audit	Identity-based	Password	Authentication token (PED Key)
Partition Security Officer	Identity-based	Password	Authentication token (PED Key)
Crypto Officer	Identity-based	Password	Authentication token (PED Key), plus optional password
Limited Crypto Officer	Identity-based	Password	Authentication token (PED Key), plus optional password
Crypto User	Identity-based	Password	Authentication token (PED Key), plus optional password
Administrator	Identity-based	Password	Authentication token (PED Key)
Public User	Not Required	N/A	N/A

Table 7: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
PED Key (if configured)	48 byte random authentication data generated when a role is initialized and stored on PED key. The probability of guessing the authentication data in a single attempt is 1 in 2^{384} (far less than 1 in 1,000,000). With a maximum of 6000 failed login attempts per minute allowed by the module (1.52 e-112, far less than 1 in 100,000), the thresholds required by FIPS 140-2 can never be reached.
Password	User provided byte array (minimum 7 bytes). The probability of guessing the challenge secret in a single attempt is 1 in 2^{56} (far less than 1 in 1,000,000). With a maximum of 6000 failed login attempts per minute allowed by the module (1.44 e-81,far less than 1 in 100,000), the thresholds required by FIPS 140-2 can never be reached.

When using the password authentication mechanism, the module encrypts a known check-word under a key derived using PBKDF from SP 800-132 and option 1a from section 5.4, 'Using the Derived Master Key to Protect Data'. During a login attempt, the module generates a key from the supplied password, and attempts to decrypt a known checkword. Successful login is achieved if the decrypted checkword matches the expected value. If successful, the PBKDF derived key is used to remove a layer of encryption from the module stored User Storage Key (USK)[4].

The length of the password used as input to the PBKDF function is consistent with the password length selected by the authenticating user which is required to be between 7 and 255 characters long. Where passwords are randomly generated, the probability of successfully guessing the password and deriving the storage key for a minimum password length of 7 characters is 1 in 2^{56}. This probability is significantly reduced if random passwords are not used.

Guidance in Appendix A, 'Security Considerations' of NIST SP 800-132 should be consulted when picking an appropriate password length in situations where encryption layers derived from the user password are required to protect the confidentiality of module protected user keys.

2.4.2 Activation

If PED authentication is configured, the Crypto-Officer, Limited Crypto Officer and Crypto-User roles can be configured to use a two-step authentication process. The first stage is termed "Activation" and is performed using a PED key. Once activated, access to key material and cryptographic services is not allowed until the second stage of authentication, 'User Login', has been performed using the role's password.

Once activated, a role stays activated until the role is explicitly deactivated, deleted or the module is reset[5].

[4] When 'decommission' is enabled as a module capability, the USK is independently encrypted in storage under a 256-bit module generated AES key.

[5] A module is reset in response to a trigger signal being received on the External Event input, Decommission signal and EFP violations, loss of power or a request from a host application.

2.4.3 M of N

If the PED based authentication is configured, the cryptographic module supports the use of an M of N (up to N=16) secret sharing authentication scheme for each of the modules roles. M of N authentication provides the capability to enforce multi-person control over the functions associated with each role.

The M of N capability uses Shamir's threshold scheme. The cryptographic module splits the randomly-generated authentication data into "N" pieces, known as splits, and stores each split on an iKey. Any "M" of these "N" splits must be transmitted to the cryptographic module by inserting the corresponding iKeys into the Luna PED in order to reconstruct the original secret.

2.5 Physical Security

The Thales Luna K7 Cryptographic Module is a multi-chip embedded cryptographic module as defined by FIPS PUB 140-2, section 4.5. The module is enclosed in a strong metal enclosure that provides tamper-evidence. Any tampering that might compromise a module's security is detectable by visual inspection of the physical integrity of a module. The HSM SO should perform a visual inspection of the module at regular intervals.

Within the metal enclosure, a hard opaque epoxy covers the circuitry of the cryptographic module. Attempts to remove this epoxy will cause sufficient damage to the cryptographic module so that it is rendered inoperable.

The module's enclosure is opaque to resist visual inspection of the device design, physical probing of the device and attempts to access sensitive data on individual components of the device.

2.5.1 External Event

The module supports a physical interface for the input of an external event signal. The external event signal jumper is monitored in both the powered-on state and the powered-off state.

In the event of an external event signal, the module will erase the Token Module Variable Key, reset itself, clear all working memory and log the event. The module can be reset and placed back into operation when the external event signal is removed.

2.5.2 PCI-E Card Removal

The module detects removal from the PCI-E slot in both the powered-on state and the powered-off state. If the card is removed from the PCI-E slot, the Token Module Variable Key (TVK) is erased and the event is logged.

2.5.3 Environmental Failure Protection

The module is designed to sense and respond to out-of-range temperature conditions as well as out-of-range voltage conditions. The temperature and voltage conditions are monitored in both the powered-on state and the powered-off state.

In the event that the module senses an out-of-range temperature or over voltage, the module will erase the TVK, reset itself, clear all working memory and log the event. The module can be reset and placed back into operation when in-bound operating conditions have been restored.

Note, under-voltage conditions are treated as a power cycle. In the event that the module senses an under voltage, the module will clear all working memory and halt operations. The TVK will not be erased. The module can be reset and placed back into operation when proper operating conditions have been restored.

2.5.4 Decommission

The module supports a physical interface for the input of a decommission signal. The decommission signal jumper is monitored in both the powered-on state and the powered-off state.

In the event of a decommission signal, the module will erase the Key Encryption Key (KEK), reset itself, clear all working memory and log the event.

This provides the capability to prevent access to sensitive objects in the event that the module has become unresponsive or has lost access to primary power.

The module can be reset, re-initialized and placed back into operation when the decommission signal is removed.

The module can optionally be configured to erase the KEK in response to the External Event signal and EFP violations described above.

2.5.5 Secure Transport Mode

Secure Transport Mode (STM) is a feature that allows the integrity of the module to be verified when the module is shipped from one location to another or placed in storage.

When a module is placed in to STM, a random string and a fingerprint of the internal state of the module is output from the module. The fingerprint is a SHA-256 digest of the random string, a randomly generated nonce, module CSPs, firmware, module configuration information and non-volatile memory. The nonce is stored in the HSE-BBRAM that is erased in response to an External Event, Decommission signal and EFP violations.

While in STM, the module is in a reduced mode of operation which only allows the module to be taken out of STM. If the module has been initialized, only the HSM SO can put the modules into STM and take it out of STM. If the HSM is in a zeroized state, only the public user can put the module into STM and take it out of STM.

The module can be taken out of STM by entering the random user string. The module will recalculate and output the fingerprint. It is the operator’s responsibility to verify that the fingerprint output matches the fingerprint initially output when the module was put in to STM.

2.5.6 Fault Tolerance

If power is lost to a module for whatever reason, the module shall, at a minimum, maintain itself in a state that it can be placed back into operation when power is restored without compromise of its functionality or permanently stored data.

A module shall maintain its secure state[6] in the event of data input / output failures. When data input / output capability is restored the module will resume operation in the state it was prior to the input / output failure.

2.6 Operational Environment

The module uses a non-modifiable operational environment. The requirements for a modifiable operating environment do not apply.

[6] A secure state is one in which either the cryptographic module is operational and its security policy enforcement is functioning correctly, or it is not operational and all sensitive material is stored in a cryptographically protected form.

2.7 Cryptographic Key Management

2.7.1 FIPS-Approved Algorithm Implementations

The FIPS-Approved algorithms implemented by the module are listed in the table below:

Table 8: FIPS-Approved Algorithm Implementation

Approved Security Functions	Certificate No.
Symmetric Encryption/Decryption	
AES: CBC, CFB128, CFB8, CTR, ECB, GCM[7], KW, KWP, OFB (128, 192, 256-bits) XTS (128 and 256-bits)	C1707.
AES: GCM[7] , KW, KWP (128, 192, 256-bits)	C1718.
Triple DES (3-key): CBC, CFB64, CFB8, CTR, ECB, OFB.	C1707.
Hashing	
SHA: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE-128, SHAKE-256 (Byte Only).	C1707.
SHA: SHA2-256, SHA2-512 (Byte Only).	C1718.
SHA: SHA-1, SHA2-384 (Byte Only).	C1701.
Message Authentication Code	
HMAC: HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512.	C1707.
HMAC: HMAC-SHA-256.	C1718.
Triple-DES: CMAC.	C1707.
AES: CMAC (128, 192, 256-bits).	C1707.

[7] The module generates IVs internally using the Approved DRBG which all IV used are 128-bits in length.

Approved Security Functions	Certificate No.
AES: GMAC (128, 192, 256-bits).	C1707, C1718.
Asymmetric	
RSA: Key Generation (2048 and 3072 modulus), Signature Generation (2048 and 3072 modulus), Signature Verification (1024, 2048 and 3072 modulus). Signature Type: ANSI X9.31, PKCS 1.5, PKCSPSS. Hash options: Signature Generation (PKCS 1.5 and PKCSPSS): SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Signature Generation (ANSI X9.31): SHA2-224, SHA2-256, SHA2-384, SHA2-512. Signature Verification (PKCS 1.5 and PKCSPSS): SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Signature Verification (ANSI X9.31): SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512.	C1707, C1717, C1718 (when using SHA-1 and SHA-2 hash options). Vendor Affirmed using FIPS IG A.11 when using SHA-3 hash.
RSA: Key Generation (2048 and 3072 modulus). Key Generation Mode: B.3.3 and B.3.6.	C1718, C1719.
RSA: Signature Generation (4096 modulus), Signature Verification (4096 modulus). Signature Type: ANSI X9.31, PKCS 1.5, PKCSPSS. Signature Generation (PKCS 1.5 and PKCSPSS): SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Signature Generation (ANSI X9.31): SHA2-224, SHA2-256, SHA2-384, SHA2-512. Signature Verification (PKCS 1.5 and PKCSPSS): SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Signature Verification (ANSI X9.31): SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512.	A480, A481 (when using SHA-1 and SHA-2). Vendor Affirmed using FIPS IG A.11 when using SHA-3.
RSA: Key Generation (4096 modulus).	A478, A479, A480, A481.
RSA: Signature Verification (4096 modulus). Hash options: SHA-1, SHA2-384.	C1701.

Approved Security Functions	Certificate No.
DSA: Parameter Generation (2048 and 3072 modulus), Key Generation (2048 and 3072 modulus), Signature Generation (2048 and 3072 modulus), Signature Verification (1024, 2048 and 3072 modulus). Hash options: Parameter Generation: SHA2-224, SHA2-256. Signature Generation: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Signature Verification: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.	C1707 (when using SHA-1 and SHA-2). Vendor Affirmed using FIPS IG A.11 when using SHA-3.
DSA: Parameter Generation (2048 and 3072 modulus), Key Generation (2048 and 3072 modulus). Hash Options: Parameter Generation: SHA2-224, SHA2-256.	C1718.
ECDSA: Key Generation, Signature Generation, Signature Generation Component (CVL), Signature Verification. Curves: B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521. Hash options: Signature Generation: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Signature Verification: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.	C1707 (when using SHA-1 and SHA-2). Vendor Affirmed using FIPS IG A.11 when using SHA-3.
ECDSA: Key Generation, Signature Generation, Signature Generation Component (CVL), Signature Verification. Curves: B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571. Hash options: Signature Generation: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Signature Verification: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.	C1718 (when using SHA-1 and SHA-2). Vendor Affirmed using FIPS IG A.11 when using SHA-3.
RSA (CVL): Decryption Primitive.	C1707, C1717, C1718, C1719.

Approved Security Functions	Certificate No.
Key Agreement Scheme	
KAS (Cert. #A480; key establishment methodology provides 256 bits of encryption strength)[8] ECC: Full Validation, Key Pair Generation Full Unified, OnePassDH. Supported curves: P-521, KDF methods: One-Step, Supported hash: SHA2-512, Key confirmation: HMAC-SHA2-512, Key length: 256, 512.	A480.
KAS-SSC[9] ECC: Ephemeral Unified, Full Unified, OnePassDH. Supported curves: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-409, B-571. Supported hash: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. FFC: dhHybrid1, dhEphem, dhHybridOneFlow, dhOneFlow. Modulus length: 2048, 3072 and 4096. Supported hash: SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.	A478, A480.
KAS-RSA (Certs #A478, #A479, #A480, #A481; key establishment methodology provides 150 bits of encryption strength)[10] KAS1-Basic: Modulus length: 4096 bits, key generation method: rsakpg1-crt, KDF method: One-Step Key Derivation from SP 800-56Cr1 using SHA2-512.	A478, A479, A480, A481.
Key Transport	
KTS (AES Certs. #C1707 and #C1718; key establishment methodology provides between 128 and 256 bits of encryption strength) AES KW and KWP(128, 192, 256-bits)	C1707, C1718.

[8] Full key agreement used by STC and with the Thales Luna PED. STC uses Full Unified Model C(2e, 2s,ECC CDH) with Bilateral Key Confirmation on P-521 with 512 bit HMAC key. Thales Luna PED (local connection) uses OnePassDH C(1e, 1s, ECC CDH) with Unilateral Key Confirmation on P-521. Thales Luna PED (remote connection) uses Full Unified Model C(2e, 2s, ECC CDH) with Bilateral Key Confirmation on P-521 with 256 bit HMAC key.

[9] Shared secret computation when requesting a Diffie-Hellman or Elliptic-Curve Diffie-Hellman key derivation using the C_DeriveKey Cryptoki API call.

[10] Full key agreement with the CPV3 protocol.

Approved Security Functions	Certificate No.
KTS-RSA (Certs. # A478, #A479, #A480 and #A481; key establishment methodology provides between 112 and 150 bits of encryption strength) KTS-OAEP-Basic: Modulus length – 2048, 3072, 4096, 6144, 8192, Hash –SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, Mask Generation Function (MGF) –SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.	A478, A479, A480, A481.
Key Derivation Function	
Key-Based Key Derivation Function (KBKDF) KDF Mode: Counter. MAC Mode: CMAC-AES128, CMAC-AES192, CMAC-AES256, CMAC TDES, HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512.	C1707 (when using SHA-1 and SHA-2). Vendor Affirmed using IG A.11 when using SHA-3.
KDA (Cert. #A480) One-Step Key Derivation using SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.	A480.
ANSI X9.42 CVL KDF Type: Concatenation Supported Hash: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.	A480.
PBKDF[11] MAC Mode: HMAC-SHA2-512	A480.
Random Number Generation	
Counter DRBG Mode: AES 256	C1707.
Key Generation	
CKG[12]	Vendor Affirmed using IG D.12.

[11] Used internal to the cryptographic module to derive the storage encryption key used to encrypt the checkword used during password based authentication. The derived key is separately used to encrypt for storage the USK which is independently also encrypted under the module generated KEK. The module uses method 1a from SP 800-132 where the derived Master Key (MK) is used directly as the Data Protection Key (DPK).

[12] Symmetric keys and seeds used for asymmetric key generation are an unmodified output from approved DRBG (Cert #C1707).

Table 9: Allowed Security Function for the Firmware Implementation

Allowed Security Functions
Key Transport
AES (key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength) (based on AES Cert. #C1707 and using allowances in FIPS IG D.9).
Triple-DES (key unwrapping; key establishment methodology provides 112 bits of encryption strength) (based on Triple-DES Cert. #C1707 and using allowances in FIPS IG D.9).
RSA (CVL Certs. #C1707, C1717, C1718 and C1719, key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength)[13] Modulus length – 2048, 3072, 4096. Hash – SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. Mask Generation Function (MGF) – SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.
Random Number Generation
NDRNG[14]

[13] Only permitted for use under FIPS IG D.9 and is not permitted for use after December 31, 2023. This entry covers the use of RSA encryption/decryption using PKCS#1-v1.5 padding which is used with CPV1 (modulus length - 2048) for transport of exchanged nonce as well as available for optional use with C_WrapKey and C_UnwrapKey user functions for import and export of secret key.

[14] the entropy source falls within a scenario of FIPS IG 7.14 that requires an entropy assessment and meets requirements of FIPS IG 7.15.

2.7.2 Non-Approved Algorithm Implementations

Non-FIPS Approved security functions are not available for use when the module has been configured to operate in FIPS-approved mode (see section 3 for further details on configuring the approved mode of operation).

> **Symmetric Encryption/Decryption**

- DES
- Triple-DES (non-compliant for encryption using 112 bit keys)
- RC2
- RC4
- RC5
- CAST3
- CAST5
- SEED
- ARIA
- SM4

> **Hashing**

- MD2
- HAS-160
- SM3
- KECCAK

> **Message Authentication Code**

- AES MAC
- DES-MAC
- RC2-MAC
- RC5-MAC
- CAST3-MAC
- CAST5-MAC
- SEED-MAC
- ARIA-MAC
- SSL3-MD5-MAC
- SSL3-SHA1-MAC
- HMAC (non-compliant for any configuration providing less than 112 bits of encryption strength)
- TUAK

- MILENAGE
- COMP128

> **Asymmetric**

- KCDSA
- RSA X-509
- RSA (non-compliant with less than 112 bits of encryption strength)
- DSA (non-compliant with less than 112 bits of encryption strength)
- ECDSA (non-compliant with less than 112 bits of encryption strength)
- EdDSA
- SM2
- EdDSA PH

> **Key Generation**

- DES
- RC2
- RC4
- RC5
- CAST3
- CAST5
- SEED
- ARIA
- GENERIC-SECRET
- SSL PRE-MASTER
- BIP32

> **Key Agreement**

- ECC (non-compliant with less than 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology; non-compliant with less than 112 bits of encryption strength)

> **Key Transport**

- RSA (key wrapping; key establishment methodology; non-compliant with less than 112 bits of encryption strength)

2.8 Critical Security Parameters

The following table lists Critical Security Parameters (CSP) used to perform approved security function supported by the cryptographic module:

Table 10: Summary of CSPs

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Key Encryption Key (KEK)	AES-256	AES-CTR DRBG	Not Input or Output.	When administrators enable Decommission, the KEK encrypts all sensitive values and is zeroized in response to a decommission signal.
Root Certificate	RSA-4096 public key certificate	Loaded at manufacturing	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the Root Key. It is self-signed with its private key controlled by Thales. Used in verifying Manufacturing Integrity Certificate (MIC) and firmware and capability updates.
Root Private	RSA-4096 private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	The root key used in the Thales controlled certificate hierarchy used by HSM to authenticate firmware/capability updates and peer HSMs in secure protocols.
Firmware Signing Key	RSA-4096 private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output	The subordinate root signing key used to certify HSM firmware updates.
Firmware Signing Certificate	RSA-4096 public key certificate	FIPS 186-4, Appendix B.3.6.	Input with Firmware Update Image which is considered plaintext.	The X.509 public subordinate certificate signed by “Root Private” signing key used to certify HSM firmware updates.
Capability Signing Key	RSA-4096 private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	The subordinate root signing key used to certify HSM capability updates.
Capability Signing Certificate	RSA-4096 public key certificate	FIPS 186-4, Appendix B.3.6.	Input with Capability Update File.	The X.509 public subordinate certificate signed by “Root Private” signing key used to certify HSM capability updates.
Manufacturer’s Integrity Certificate (MIC)	RSA-4096 public key certificate	Loaded at manufacturing	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the Manufacturing Integrity Key (MIK) controlled by Thales. It is signed by the Root Key. Used in verifying all key material certified by Hardware Origin Certificates (HOCs).
Manufacturer’s Integrity Key	RSA-4096 private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	The subordinate root signing key used to certify HSM Hardware Origin Keys.
ECC Manufacturing Integrity Certificate (ECC MIC)	ECC public certificate for public key on curve P-384.	Loaded at manufacturing	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the ECC Manufacturing Integrity Key (ECC MIK). It is self-signed.
ECC Manufacturer’s Integrity Key	ECC private key on curve P-384	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	The subordinate root signing key used to certify HSM ECC Hardware Origin Keys.
Hardware Origin Key (HOK)	RSA 4096 bit private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	A 4096 bit RSA private key used to sign certificates for other device key pairs, such as the TWC4 used with CPV3. It is generated at the time the device is manufactured.
Hardware Origin Certificate (HOC)	RSA-4096 public key certificate	Loaded at manufacturing	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the HOK. It is signed by the Manufacturer’s Integrity Key (MIK) at the time the device is manufactured. Used in verifying all key material signed by the HOK.
FM Hardware Origin Key (FM HOK)	RSA 4096 bit private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	A 4096 bit RSA private key used to sign certificates for other device key pairs, such as the TWC4. It is generated at the time the device is manufactured.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
FM Hardware Origin Certificate (FM HOC)	RSA-4096 public key certificate	Loaded at manufacturing	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the FM HOK. It is signed by the Manufacturer's Integrity Key (MIK) at the time the device is manufactured. Used in verifying all key material signed by the FM HOK.
ECC Hardware Origin Key (ECC HOK)	ECC private key on curve P-384	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	ECC P-384 private key used to sign other device keys and used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
ECC Hardware Origin Certificate (ECC HOC)	ECC public certificate for public key on curve P-384.	FIPS 186-4, Appendix B.4.1.	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the ECC HOK. It is signed by the ECC Manufacturing Integrity Key (ECC MIK). It is used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
FM ECC Hardware Origin Key (FM ECC HOK)	ECC private key on curve P-384	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	ECC P-384 private key used to sign other device keys and used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
FM ECC Hardware Origin Certificate (FM ECC HOC)	ECC public certificate for public key on curve P-384.	FIPS 186-4, Appendix B.4.1.	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the FM ECC HOK. It is signed by the ECC Manufacturing Integrity Key (ECC MIK). It is used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
Token or Module Unwrapping Key (TUK3)	RSA-2048 bit private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	A 2048-bit RSA private key used with the Cloning Protocol Version 1 supported for key import only. It is following initial request for the key.
Token or Module Wrapping Certificate (TWC3)	RSA-2048 public key certificate	FIPS 186-4, Appendix B.3.6.	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the TUK4. It is signed by the HOK. Used in exchange of nonce (KEVs and KEVt) as part of the handshake during the cloning protocol version 1 supported for key import only.
Token or Module Unwrapping Key (TUK4)	RSA-4096 bit private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	A 4096 bit RSA private key used in the key cloning protocol. It is generated each time the module initializes from power up or reset.
Token or Module Wrapping Certificate (TWC4)	RSA-4096 public key certificate	FIPS 186-4, Appendix B.3.6.	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the TUK4. It is signed by the HOK. Used in exchange of nonce (KEVs and KEVt) as part of the handshake during the cloning protocol.
Cloning Key Encryption Vector – source (KEV^s)	384 bit nonce.	AES-CTR DRBG	Exchanged during CPV1 and CPV3 protocol (see section 2.8.2 for further details).	384 bit nonce used with the cloning protocol and generated on the source HSM.
Cloning Key Encryption Vector – target (KEV$_t$)	384 bit nonce.	AES-CTR DRBG	Exchanged during CPV1 protocol (see section 2.8.2 for further details).	384 bit nonce used with the cloning protocol and generated on the target HSM.
Cloning Transfer Key	AES-256	Single Step Concatenation KDF from NIST SP 800-56Cr1 and SHA2-512 as hash.	Not Input or Output.	256 bit AES key derived during the cloning protocol and used to transfer key objects between source and target partitions using the cloning protocol.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Device Authentication Key (CITS-DAK)	RSA 4096 private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	4096-bit RSA private key used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
Device Authentication Key (CITS-DAC)	RSA-4096 public key certificate	FIPS 186-4, Appendix B.3.6.	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the CITS-DAK. Signed by the HOK. Used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
ECC Device Authentication Key (ECC DAK)	ECC private key on curve P-384	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	ECC P-384 private key.
ECC Device Authentication Certificate (ECC DAC)	ECC public certificate for public key on curve P-384.	Loaded at manufacturing	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the ECC DAK. It is signed by the ECC HOK.
Token or Module Variable Key (TVK)	AES-256	AES-CTR DRBG	Not Input or Output.	It is used to encrypt authentication data stored for auto-activation purposes.
Secure Transport Mode (STM) Nonce	992-bits	AES-CTR DRBG	Not Input or Output.	Random value used to create module fingerprint that is used to verify the module's integrity as part of the Secure Transport Mode feature.
DRBG Key	AES-256	Hardware Noise Source	Not Input or Output.	32 bytes AES key stored in the RAM. Used in an implementation of the NIST SP 800-90Ar1 CTR (AES) DRBG.
DRBG Seed	384 bits	Hardware Noise Source	Not Input or Output.	Random seed data drawn from the Hardware RBG and used to seed an implementation of the NIST SP 800-90Ar1 CTR (AES) DRBG.
DRBG V	128 bits	Hardware Noise Source	Not Input or Output.	Part of the secret state of the approved DRBG. The value is generated using the methods described in NIST SP 800-90Ar1.
DRBG Entropy Input	384 bits	Hardware Noise Source	Not Input or Output.	The 384-bit entropy value used to initialize the approved DRBG.
Global Storage Key (GSK)	AES-256	AES-CTR DRBG	Not Input or Output.	32-byte AES key that is the same for all users on a specific Luna cryptographic module. It is used to encrypt permanent parameters within the non-volatile memory area reserved for use by the module.
Role Domain Key (RDK)	48-byte random value (PED configuration) Or 7 - 255 character data string (Password configuration).	AES-CTR DRBG for PED configuration. N/A for Password configuration.	Input / Output via direct connection to PED.	For PED configurations, this is a 48-byte value, the first 32-bytes of which are used as an AES KW 256-bit key that is used to wrap/unwrap the SALK when it is exported / imported from / to the module. It is either generated by the module or imprinted onto the module at the time Audit role is initialized. The value is output from the original module onto a PED key to enable initializing the Audit role on additional modules into the same domain. For password configurations, this value is supplied by the user during configuration of the secure audit capability.
Secure Audit Logging Key (SALK)	256 bit HMAC key	AES-CTR DRBG	Input / Output encrypted under the RDK and using AES-256 in KWP mode.	A 256-bit key used to verify data integrity and authentication of the log messages. Saved in the parameter area of Flash memory.
Secure Audit AppID-HMAC Key	256 bit HMAC key	AES-CTR DRBG	Not Input or Output.	A 256-bit key used to create an HMAC of the AppID to be used in the Secure Audit logs, to prevent against the theft of the actual AppID. A new key will be generated at every module power-on or firmware reset.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
User Password (if PED configuration and optionally selected)	7 - 64 character data string	N/A	Input from host using ICD communication path and encrypted under the PEC and using KTS-OAEP-basic from SP 800-56Br2.	User provided password input by the operator as a second factor of authentication data.
PED Authentication Data (if PED configuration)	48-byte random value	AES-CTR DRBG	Input / Output via direct connection to PED. All messages sent to the local PED are encrypted using	A 48-byte random value that is generated by the module when a role is created and is written out to the PED key via the Trusted Path.
Password (Authentication Data if Password configuration)	7 - 255 character data string	N/A	Input from host using ICD communication path and encrypted under the PEC and using KTS-OAEP-basic from SP 800-56Br2.	User provided password input by the operator as authentication data. The password is input to the PBKDF in order to derive a key used to decrypt a known checkword alongside the USK as part the authentication process (the USK is separately also encrypted under the KEK when decommission is enabled).
User Storage Key (USK)	AES-256	AES-CTR DRBG	Not Input or Output.	This key is used to encrypt all sensitive attributes of all private objects owned by the User.
Partition Storage Key (PSK)	AES-256	AES-CTR DRBG	Not Input or Output.	This key is unique per-partition and used to encrypt all CSP that are shared by all roles of a given partition.
SKS Master Key (SMK)	AES-256	AES-CTR DRBG	Input/Output using CPV3. Input for key migration purposes using CPV1.	A randomly generated 256-bit secret used as the master key for deriving all SKS key blob encryption keys.
HA Login Public Key (HA_{PUB})	4096-bit public key	FIPS 186-4, Appendix B.4.1.	Certificate Output in Plaintext.	A 4096-bit RSA public key used for the HA Login protocol.
HA Login Private Key (HA_{PK})	4096-bit private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	A 4096-bit RSA private key used for the HA Login protocol.
HA Login Authentication Data Encryption Key PIN (RND)	AES-256	AES-CTR DRBG	Output encrypted using AES-256 in KWP mode and using a shared secret from output of SP 800-56Br2, KAS1-Basic exchange.	An AES 256-bit encryption key used to encrypt authentication data for export to the primary HA Login instance.
HA Login Ephemeral Wrapping Key (K_{SESS})	AES-256	AES-CTR DRBG	Output encrypted with peer TWC.	An AES 256-bit encryption key used to encrypt authentication data for re-import from the primary HA Login instance.
Key Cloning Domain Vector (KCV)	48-byte random value (PED configuration) Or 7 - 255 character data string (Password configuration).	AES-CTR DRBG for PED configuration. N/A for Password configuration.	Input / Output via direct connection to Thales PED.	Value that controls a partition's ability to participate in the cloning protocol. In the case of PED configurations, it is generated by the module or imprinted onto the module at partition initialization time. For password configurations, this value is supplied by the user during partition initialization. For PED configurations, the value is output from the original partition in the domain to a PED key to enable initializing additional modules into the domain.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Remote PED Vector (RPV) (if PED configuration)	256-bit secret value	AES-CTR DRBG	Output via direct connection to a Luna PED.	A randomly generated 256-bit secret, which must be shared between a remote PED and a cryptographic module in order to establish a secure communication channel between them.
PED Authentication Certificate (PAC)	ECC public key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	An ECC public key certificate used to verify certificates for local or remote connection with a Luna PED.
PED Authentication Key (PAK)	ECC private key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	An ECC private key used to sign certificates used for local or remote connection with the Luna PED.
HSM Static Key-Agreement Certificate for Local Connections (HSM-SKA-C_{LOCAL})	ECC public key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	Used by the Luna PED to authenticate the local HSM to connect to and to extract the HSM's static ECC public key for C(1e,1s, ECC CDH) key-agreement for local connection with a Luna PED.
HSM Static Key-Agreement Private Key for Local Connections (HSM-SKA-K_{LOCAL})	ECC private key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	Used by the HSM as the static private key for C(1e,1s, ECC CDH) key-agreement agreement for local connection with a Thales Luna PED.
HSM Static Key-Agreement Certificate for Remote Connections (HSM-SKA-C_{REMOTE})	ECC public key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	Used by the PED to authenticate the remote HSM to connect to and to extract the HSM's static ECC public key for: • C(2e,2s, ECC CDH) key-agreement for remote connection with PED. • C(1e,1s, ECC CDH) DLC Key Transport for CSP migration
HSM Static Key-Agreement Private Key for Remote Connections (HSM-SKA-K_{REMOTE})	ECC private key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	Used by the remote HSM as the static private key for: • C(2e,2s, ECC CDH) key-agreement agreement for remote connection with PED. • C(1e,1s, ECC CDH) DLC Key Transport for CSP migration
HSM Ephemeral Key-Agreement Certificate (HSM-EKA-C)	ECC public key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	Used by the Luna PED to authenticate the remote HSM to connect to and to extract the HSM's ephemeral public key for C(2e,2s, ECC CDH) key-agreement agreement for remote connection with a Luna PED.
HSM Ephemeral Key-Agreement Private Key (HSM-EKA-K)	ECC private key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Not Input or Output	Used by the Luna PED to authenticate the remote HSM and to extract the HSM's ephemeral public key for C(2e,2s, ECC CDH) key-agreement agreement for remote connection with a Luna PED.
Remote PED Vector Certificate (RPV-C)	ECC public key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	An ECC public key certificate used by the HSM device to verify PED-SKA-C, PED-EKA-C.
Remote PED Vector Private Key (RPV-K)	ECC private key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	An ECC private key used by the HSM to sign PED-SKA-C, and by the Luna PED to sign PED-EKA-C.
PED Static Key-Agreement Certificate for Remote Connections (PED-SKA-C)	ECC public key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	Used by the HSM to authenticate and extract the Luna PED's ECC ephemeral public key for C(2e,2s, ECC CDH) or C(1e,1s ECC CDH) key-agreement. Uniquely generated for each use.
PED Static Key-Agreement Private Key (PED-SKA-K)	ECC private key on curve P-521.	FIPS 186-4, Appendix B.4.1.	Output via direct connection to a Luna PED.	Used by the Luna PED for Remote connections. Act as An ECC static private key for C(2e,2s, ECC CDH) key-agreement. Key isn't used by the HSM as a CSP but is generated by it for use by the Luna PED.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
HSM CSP Wrapping Key (CWK_{HSM})	AES-256	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Local and Remote PED Channel for wrapping exchanged CSPs.
PED CSP Wrapping Key CWK_{PED}	AES-256	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Local and Remote PED Channel for wrapping exchanged CSPs.
HSM Data Encryption Key (DEK_{HSM})	AES-256	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Remote PED Channel for encrypting communication messages (from HSM-to-PED).
HSM MAC Key (DMK_{HSM})	256 bits	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Remote PED Channel for message authentication of communication messages (from HSM-to-PED).
HSM Initialization Vector (IV_{HSM})	256 bits	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Remote PED Channel as the initialization vector for encrypting communication messages (from HSM-to-PED).
PED Data Encryption Key (DEK_{PED})	AES-256	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Remote PED Channel for encrypting communication messages (from PED-to-HSM).
PED MAC Key (DMK_{PED})	256 bits	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Remote PED Channel for message authentication of communication messages (from PED-to-HSM).
PED Initialization Vector (IV_{PED})	256 bits	Single Step Concatenation KDF from NIST SP 800-56Cr1 and using SHA2-512 as hash.	Not Input or Output.	Derived during Remote PED Channel as the initialization vector for encrypting communication messages (from PED-to-HSM).
Password Encryption Key (PEK)	RSA 4096 bit private key	FIPS 186-4, Appendix B.3.6.	Not Input or Output.	A 4096 bit RSA private key used to decrypt user passwords that are provided to the module. It is generated the first time it is required.
Password Encryption Certificate (PEC)	RSA-4096 public key certificate	FIPS 186-4, Appendix B.3.6.	Certificate Output in Plaintext.	The X.509 public key certificate corresponding to the PEK. It is created and signed by the HOK the first it is required.
Partition STC Static Public ID Key ($STC\text{-}PID_{PUB}$)	ECC public key on curve P-521	FIPS 186-4, Appendix B.4.1.	Certificate Output in Plaintext.	A 521-bit ECC public key used as the partition's static ID in the STC protocol.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Partition STC Static Private ID Key (STC-PID$_{PRIV}$)	ECC private key on curve P-521	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	A 521-bit ECC private key used as the partition's static ID in the STC protocol.
Partition STC Ephemeral Public Key (STC-PKA$_{PUB}$)	ECC public key on curve P-521	FIPS 186-4, Appendix B.4.1.	Certificate Output in Plaintext.	A 521-bit ECC public key used as the partition's ephemeral key in the STC protocol.
Partition STC Ephemeral Private Key (STC-PKA$_{PRIV}$)	ECC private key on curve P-521	FIPS 186-4, Appendix B.4.1.	Not Input or Output.	A 521-bit ECC private key used as the partition's ephemeral key in the STC protocol.
Client STC Static Public ID Key (STC-CID$_{PUB}$)	ECC public key on curve P-521	External	Input in Plaintext.	A 521-bit ECC public key used as the client's static ID in the STC protocol.
Client STC Ephemeral Public Key (STC-CKA$_{PUB}$)	ECC public key on curve P-521	External	Input in Plaintext.	A 521-bit ECC public key used as the client's ephemeral key in the STC protocol.
Partition STC Session Encryption and Authentication Keys (STC-PEN, STC-PMA, STC-PIV, STC-CEN, STC-CMA, STC-CIV)	AES-128 HMAC-SHA512	NIST SP 800-56Ar3 key agreement.	Not Input or Output.	These keys are agreed upon with a client application for the purpose of encrypting and generate MAC for message exchanges during an STC session.
Asymmetric Key Pairs (general partition or session keys)	RSA, DSA, ECC, DH	N/A (user imported) or either FIPS 186-4, Appendix B.3.3 or B.4.1.	Input or output encrypted using Symmetric Keys (general partition or session keys) using key wrap/unwrap ICD commands using key wrap/unwrap ICD commands and SP 800-38F encryption options. Input using Symmetric Keys (general partition or session keys) using key unwrap ICD commands and approved symmetric algorithms as permitted by FIPS IG D.9. When transferred between partitions using SKS, encrypted under the SMK. Input using CPV1 as covered in section 2.8.2.	General use asymmetric key pairs that can be exported/imported from/to the module or generated by the module.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Symmetric Keys (general partition or session keys)	AES or TDES (including AES-XTS), MAC, KDF.	N/A (user imported) or AES-CTR DRBG (module generated).	Input or output encrypted using Symmetric Keys (general partition or session keys) using key wrap/unwrap ICD commands and SP 800-38F encryption options. Input or output encrypted using Asymmetric Keys (general partition or session keys) using key wrap/unwrap ICD commands and KTS-OAEP-basic from SP 800-56Br2. Input using Symmetric Keys (general partition or session keys) using key unwrap ICD commands and approved symmetric algorithms as permitted by FIPS IG D.9. When transferred between partitions using SKS, encrypted under the SMK. Input using CPV1 as covered in section 2.8.2.	General use asymmetric key pairs that can be exported/imported from/to the module or generated by the module.

2.8.1 Key Generation

Symmetric cryptographic keys are generated by the direct unmodified output of the module's NIST SP 800-90Ar1 DRBG. The DRBG output is also used to provide seeds for asymmetric key generation.

Keys which are generated outside the module and input during the manufacturing process include: Root Certificate, MIC and ECC MIC.

The HOC, ECC HOC, FM HOC and FM ECC HOC are created outside the module during manufacture based on public keys generated by the module and exported as part of the manufacturing process. Once signed by corresponding externally managed keys, these are re-loaded onto the module for subsequent validation and storage.

User passwords for authentication of roles are generated by the operator.

The NIST SP 800-90Ar1 DRBG (CTR-DRBG using AES-256) is seeded using 2048 bits or raw entropy taken from the module NDRNG which is conditioned using SHA-512 ahead of creating the 384 bit seed. Based on calculated min-entropy values for the platform raw noise source and factors outlined in NIST SP 800-90B, the 384-bit input used to seed to the DRBG has a full 384 bits of entropy.

2.8.2 Key Import and Export

Import and Export of CSP is supported over the following interface:

> Physical Trusted Path (local PED); or

> Luna ICD, logical interface**.**

For details of specific mapping of CSP to interfaces and associated methods of encryption of specific CSP refer to the Input / Output column of Table 10.

Depending on the configuration of the module, the following methods of key import and export for 'Asymmetric Key Pairs (general partition keys)' and 'Symmetric Keys (general partition keys)' are available as a service:

> **Key Wrap / Unwrap using Cloning Protocol Version 3 (CPV3)**

Cloning is a product feature where KAS1-Basic from SP 800-56Br2 is used to negotiate a shared secret used to transfer partition objects between a source and destination partition and where these can be on the same or different cryptographic module. The protocol uses the following options with KAS1-Basic:

- RSASVE for transfer of shared secrets uses the public key from the TWC4 certificate which has a modulus length of 4096 bits;
- Shared keys are derived using One-Step KDF from SP 800-56Cr1 using SHA2-512. Inputs to the KDF include the exchanged shared secret from the RSASVE transfer, alongside the pre-shared 256 bit secret key (KCV or RDK) and additional HSM related shared information; and
- Encryption of the SMK during the transfer uses AES-256 in KWP mode and a single-use key and IV derived from the output of the KDF.

> **Scalable Key Storage (SKS)**

SKS allows the transfer of partition objects (symmetric and asymmetric keys, alongside other objects) between partition encrypted under the SMK which must have been pre-shared between source and destination partition using CPV3.

SKS uses AES-256 in GCM mode with a 128bit random IV generated by the cryptographic module using output from its NIST SP 800-90Ar1 DRBG and where a unique key per extraction is used. This key is deriver using the shared partition SMK and a 256-bit random salt value (unique per SKS export operation) and the SMK.

Encryption keys are derived using SP 800-108 PRF KDF and using AES-CMAC-256.

> **Key Wrap / Unwrap**

The key wrap operation is available for use to import or export raw Symmetric Keys (general partition or session keys) or an Asymmetric Key Pair (general partition or session keys) – private key, using one of the following options:

- KTS-OAEP-basic from SP 800-56Br2 and where the following options are supported:
  - Modulus lengths of 2048, 3072 or 4096 (for export) or 1024, 2048, 3072 and 4096 for import;
  - Hash and MGF options must match and be consistent with one of the following algorithms: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512.
- SP 800-38F compliant KTS using one of the following options for both key unwrapping and wrapping:
  - AES (128, 192 or 256) in KW, KWP;
- FIPS IG D.9 compliant KTS for unwrap of key objects using one of the following options:
  - AES (128, 192 or 256) in CBC, CTR or ECB modes; or
  - TDES (112 and 168 bit) in CBC, ECB and CTR.

The unwrap operation takes as input an encrypted symmetric key or asymmetric private key and a handle to the key required to successfully unwrap the object. It decrypts the key and returns the handle to the imported key.

> **Key Unwrap using Cloning Protocol Version 1 (CPV1)**

CPV1 is supported to enable the import of keys from existing Thales HSM with firmware prior to 7.7.0 to the cryptographic module.

CPV1 operates in the following way:

- 256 bit nonce (KEV_t and KEV_s) are transferred using RSA with PKCSv1.5 encryption and the public key from the TWC3 certificate (of source and destination partitions) with modulus length of 2048 bits.
- Shared keys are derived using One-Step KDF from SP 800-56Cr1 using SHA2-512 and with the source and destination nonce (KEV_t and KEV_s) alongside KCV (or RDK) as inputs. KCV (or RDK) are transferred out of band of the protocol to source and destination partitions either as a pre-shared password or on the red PED key presented using the Luna PED.
- Encryption of the partitions object during transfer uses AES-256 in CBC mode alongside having an independent SHA2-256 hash for integrity protection.

> **Key Unwrap using historic versions of SKS**

The module supports key import for keys previously exported from other FIPS certified Thales HSM using versions of SKS supported by legacy firmware versions and where related certificates are now on NIST's historical list.

Import is supported for key migration only and where ahead of import, the SMK used to originally encrypt the object must be transferred to the target partition using CPV1.

Objects imported using this method are either:

- Encrypted using AES-256 in GCM mode with SHA256 for integrity protection; or
- Encrypted using AES-256 in OFB mode and with SHA1 for integrity protection;

2.8.3 Limits on the use of TDES keys

In conformance with limitations on the maximum number of blocks encrypted for a given 168-bit TDES key outlined in SP 800-67r1 and further tightened in FIPS IG A.13 ‘SP 800-67rev1 Transition’ – the cryptographic module technically enforces that any given TDES key stored in the cryptographic module cannot be used for more than 2^{16} 64-bit data block encryption operations.

TDES keys created on the HSM (imported or generated) include a ‘remaining blocks’ attribute that is managed by the HSM and decremented following each encrypt operation requested. Once the ‘remaining blocks’ count reaches zero, the key is permitted for use with decrypt and MAC verify operations exclusively and is prohibited from being copied, exported and/or for the counter being reset to a non-zero value.

2.9 Self-Tests

2.9.1 Power-On Self-tests

The module performs Power-On Self-Tests (POST) upon power-up to confirm the firmware integrity, and to check the continued correct operation of the random number generator and each of the implemented cryptographic algorithms. While the module is running POST, all interfaces are disabled until the successful completion of the self tests. If any POST fails an error message is output, the module halts, and data output is inhibited.

These self-tests can also be initiated as an operator service but do not require operator input to initiate at power on.

Table 11: Power On Self-Tests (Bootloader) – Module Integrity

Test	When Performed	Indicator
Boot loader performs an RSA 4096-bit SHA2-384 signature verification of itself	Power-on	Error output and module halt
Boot loader performs an RSA 4096-bit SHA2-384 signature verification of the firmware prior to firmware start	Power-on/Request[15]	Error output and module halt
SHA (SHA-1 and SHA2-384) and RSA (4096 modulus) KAT.	Power-on/Request[16]	Error output and module halt

[15] Request indicates triggering a POST via a command

[16] Request indicates triggering a POST via a command

Table 12: Power On Self-Tests (Firmware) – Cryptographic Implementations

Test	When Performed	Indicator
DRBG Self-Test (Instantiate Function Known Answer Test, Generate Function KAT, Reseed Function KAT, conditional tests)	Power-on/once every 24 hours.	Error output and module halt
SHA KAT (SHA1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE-128, SHAKE-256)	Power-on/Request	Error output and module halt
HMAC KAT (HMAC-SHA1, HMAC-SHA224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512)	Power-on/Request	Error output and module halt
RSA KAT (Signature Generation, Signature Verification, Encrypt, Decrypt)	Power-on/Request	Error output and module halt
DSA KAT (Signature Generation, Signature Verification)	Power-on/Request	Error output and module halt
Diffie-Hellman KAT (X9.42 DH Derive)	Power-on/Request	Error output and module halt
AES KAT (ECB, CBC, OFB, CFB, CFB128, CFB8, KW, KWP, GCM, XTS modes covering 128, 192 and 256 bit keys, CMAC and GMAC).	Power-on/Request	Error output and module halt.
Triple-DES KAT (ECB, CBC, OFB, CFB64 (162 bit keys), CTR, CMAC).	Power-on/Request	Error output and module halt.
ECDH KAT (Derive)	Power-on/Request	Error output and module halt
ECDSA KAT (Signature Generation, Signature Verification)	Power-on/Request	Error output and module halt.
KBKDF KAT (SP 800-108 KBKDF using AES-CMAC, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 as PRF).	Power-on/Request	Error output and module halt.
KDF KAT (SP 800-56Cr2 One-Step KDF using SHA1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512).	Power-on/Request	Error output and module halt.
KAS1-basic KAT (SP 800-56Br2 using 4096-bit RSA modulus)	Power-on/Request	Error output and module halt.
PBKDF KAT (SP 800-132)	Power-on/Request	Error output and module halt.

2.9.2 Conditional Self-Tests

The module automatically performs conditional self-tests based on the module operation. These self-tests do not require operator input to initiate.

Table 13: Conditional Self-Tests

Test	When Performed	Where Performed	Indicator
NDRNG conditional tests[17]	Continuous	Firmware / Hardware	Error output and module halt
HRNG conditional tests	Continuous	Firmware / Hardware	Error output and module halt
RSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output
DSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output
ECDSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output
Firmware load test (4096-bit RSA Signature Verification)	On firmware update load	Firmware	Error output – module will continue with existing firmware

2.10 Mitigation of Other Attacks

Timing attacks are mitigated directly by a module through the use of hardware accelerator chips for modular exponentiation operations. The use of constant timing hardware acceleration ensures that all RSA signature operations complete in the same time, therefore making the analysis of timing differences irrelevant. RSA blinding may also be enabled as an additional defense in depth optional mitigation.

[17] CRNGT, as described in Section 4.9.2 of FIPS 140-2, is only performed for the NDRNG and is not performed for the DRBG as permitted by FIPS IG 9.8 for modules implementing an approved DRBG from NIST SP 800-90Ar1.

3 Guidance

3.1 Identifying the Module Version

Ahead of putting the module into its approved mode of operation, it is important to identify the hardware, firmware and bootloader versions of the target module and to check these correspond to those listed in section 1.2. The following sections provide guidance on checking each element.

Any module returning hardware, firmware and bootloader versions not listed in this security policy is out of the scope of this validation and requires a separate FIPS 140-2 certificate.

3.1.1 Checking the Bootloader and Firmware Version

Two paths are supported to checking the hardware, bootloader and firmware versions depending on whether the LunaCM or LUSH management interfaces are being used[18]:

- **`hsm showinfo`** when using LunaCM; or
- **`hsm show`** when using LunaSH.

See section 3.1.2 for steps to verify the firmware build.

All commands return status information on the target cryptographic module including the version numbers for both bootloader and firmware and separately the hardware identity.

Example output for each command for a valid module is shown in the Figure **4**, Figure 5, Figure 6, Figure 7, and Figure 8 below with relevant versions highlighted in red:

lunacm:>hsm showinfo

```
        Partition Label -> myPCIeHSM
        Partition Manufacturer -> SafeNet
        Partition Model -> Luna K7
        Partition Serial Number -> 67842
        Partition Status -> L3 Device
         HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_RNG
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> Not Supported
        Slot Id -> 4
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 000000000000000002090100

        Partition Storage:
                Total Storage Space:  393216
                Used Storage Space:   0
                Free Storage Space:   393216
                Object Count:         0
```

[18] Both LunaCM and LunaSH map to the Luna ICD logical interface at the cryptographic module boundary.

```
        Overhead:              9848

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

FM HW Status ->          FM
 Bootloader Version -> 1.1.5
 Firmware Version -> 7.7.1
Rollback Firmware Version -> 7.0.3

Environmental:
        Fan 1 Status                            : active
        Fan 2 Status                            : active
        Battery Voltage                         : 3.093 V
        Battery Warning Threshold Voltage       : 2.750 V
        System Temp                             : 38 deg. C
        System Temperature Warning Threshold    : 75 deg. C

HSM Storage:
        Total Storage Space:   33554432
        Used Storage Space:    33554432
        Free Storage Space:    0
        Allowed Partitions:    1
        Number of Partitions: 1

License Count -> 8
        1. 621000068-000 K7 Base Configuration
        2. 621010185-003 Key backup via cloning protocol
        3. 621000135-002 Enable allow decommissioning
        4. 621000134-002 Enable 32 megabytes of object storage
        5. 621000154-001 Enable decommission on tamper with policy off
        6. 621000021-002 Maximum performance
        7. 621000138-001 Controlled tamper recovery
        8. 621000074-001 Enable Functionality Modules

Command Result: No Error
```

Figure 4: Example output of `hsm showinfo` command from LunaCM

```
lunash:>hsm show

        Appliance Details:
        ==================
        Software Version:               7.7.0-1

        HSM Details:
        ============
        HSM Label:                         myLunaHSM
        Serial #:                          66331
        Bootloader:                          1.1.5
        Firmware:                            7.7.1
        HSM Model:                         Luna K7
        HSM Part Number:                     808-000073-003
        Authentication Method:             Password
        HSM Admin login status:            Not Logged In
        HSM Admin login attempts left:     3 before HSM zeroization!
        RPV Initialized:                   No
        Audit Role Initialized:            No
        Remote Login Initialized:          No
        Manually Zeroized:                 No
        Secure Transport Mode:             No
        HSM Tamper State:                  No tamper(s)

        Partitions created on HSM:
```

```
   ==============================
   Partition:         154438865296, Name: mypar0

   Number of partitions allowed:        100
   Number of partitions created:        1

   FIPS 140-2 Operation:

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

   HSM Storage Information:
   ========================
   Maximum HSM Storage Space (Bytes):   33554432
   Space In Use (Bytes):                335544
   Free Space Left (Bytes):             33218888


   Environmental Information on HSM:
   =================================
   Battery Voltage:                     3.072 V
   Battery Warning Threshold Voltage:   2.750 V
   System Temp:                         53 deg. C
   System Temp Warning Threshold:       75 deg. C


   Functionality Module HW:            FM
   =======================

Command Result : 0 (Success)
```

Figure 5: Example output of `hsm show` command from LunaSH

3.1.2 Checking Firmware Build Version

To check the firmware release version to differentiate between FW 7.7.1 and FW build 7.7.1-20, use:

1. `hsm supportinfo` when using LunaSH on Thales Luna Network HSM.
2. `./lunadiag` for Thales Luna PCIe running Linux; or
3. `lunadiag.exe` from a Windows command line.

The `hsm supportinfo` command will generate a .txt file that must be opened to view the information.

lunash:>hsm supportInfo

```
'hsm supportInfo' successful.

Use 'scp' from a client machine to get file named:
supportInfo.txt
```

From the text file:

```
=====================================================================
        HOST INFORMATION and DATE/TIME
=====================================================================

Wed Nov 2 15:02:37 EDT 2022
local_host
```

```
=====================================================================
        BACKUP TOKEN INFO AND POLICIES
=====================================================================

   No backup token present.

=====================================================================
        HSM INFO
=====================================================================


   HSM Details:
   ============
   HSM Label:                           Pri_SA1
   Serial #:                            593658
   Bootloader:                              1.1.5
   Firmware:                                7.7.1
   HSM Model:                           Luna K7
   HSM Part Number:                     808-000073-001
   Authentication Method:               Password
   HSM Admin login status:              Not Logged In
   HSM Admin login attempts left:       3 before HSM zeroization!
   RPV Initialized:                     No
   Audit Role Initialized:              No
   Remote Login Initialized:            No
   Manually Zeroized:                   No
   Secure Transport Mode:               No
   HSM Tamper State:                    No tamper(s)
```

Figure 6: Example output of `hsm supportinfo` showing the base bootloader and firmware versions

To find the firmware build number, search the text file for the text `FW Rev` In the below example, 7.7.1 is the firmware version and **-**`20` is the build number.

```
Entry   25, 0x3d bytes read, timestamp = 21292, reset count = 12:
LOG(INFO):     HSM core init complete: online
Entry   26, 0x2e bytes read, timestamp = 380, reset count = 13:
LOG(INFO):      FW Rev 7.7.1-20
Entry   27, 0x43 bytes read, timestamp = 380, reset count = 13:
LOG(INFO):     File: ./SOURCE/LUNA2/MAIN_MOD/main.c
```

Figure 7: Example output of `hsm supportinfo` showing in addition the specific build

Use of the lunadiag tool also requires searching for `FW Rev`. To display the firmware, follow the following steps:

1. Execute the `./lunadiag` command (in Linux) or `lunadiag.exe` (in a command line in Windows).
2. Enter the slot number where the K7 card resides
3. Select option `18 Read Diagnostic Log`
4. Select option `7 Software Info`
5. To find the firmware build number, search output file for the text `FW Rev`. In the below example, 7.7.1 is the firmware version and `-20` is the build number.

```
Entry    9, 0x49 bytes read, timestamp = 70022, reset count = 6:
LOG(INFO):     Deactivating (erasing the TVK in NVRAM)...
Entry   10, 0x2e bytes read, timestamp = 371, reset count = 7:
LOG(INFO):      FW Rev 7.7.1-20
Entry   11, 0x43 bytes read, timestamp = 372, reset count = 7:
LOG(INFO):     File: ./SOURCE/LUNA2/MAIN_MOD/main.c
```

Figure 8: Example excerpt of output from `lunadiag option 7` **showing the firmware revision and build**

3.2 Approved Mode of Operation

To place the module in FIPS 140-2 Approved mode, the HSM Security Officer must check and, if necessary, set the following HSM level policies:

- HSM Policy (12), “Allow Non-FIPS Algorithms” – this is enabled by default and shall be disabled;
- HSM Policy (50), “Allow Functionality Modules” – this is disabled by default and shall either remain disabled or shall be disabled to enter FIPS mode;

If the HSM Security Officer attempts to enable or disable these policies, a warning is displayed and the HSM Security Officer is prompted to confirm the selection. If either of these policies are left (or put) in the “enabled” state, the module will be operating in the non-Approved mode.

As a confirmation and secondary step - The HSM Security Officer can independently confirm that the cryptographic module is in FIPS 140-2 Approved mode by executing the status commands covered in the prior section. Confirmation of FIPS mode status is provided on the lines highlighted in green on Figure 4 and Figure 5.

Where the modules configuration has not met the above requirements the following alternative statement will be found in the output of these comments:

```
The HSM is not in FIPS 140-2 approved operation mode.
```

Following entry into an approved mode of operation – any changes to HSM Policy (12) or HSM Policy (50) will trigger an automatic zeroization of the HSM erasing all roles and partition stored key objects.