THALES

Thales Luna Backup HSM Cryptographic Module

NON-PROPRIETARY SECURITY POLICY

FIPS 140-2, LEVEL 3

Document Information

Document Part Number	002-000148-001
Release Date	March 31, 2022

Revision History

Revision	Date	Reason
B	December 1, 2021	Initial release.
C	September 14, 2021	Updates to address CMVP coordination.
D	December 1, 2021	Additional algorithm certificates added.
E	February 9, 2022	Addressed comments from CMVP coordination. Added new hardware part number 808-000064-006.
F	March 31, 2022	Addressed comments from CMVP coordination surrounding key strength caveats.

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

Acronyms and abbreviations

Term	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
BBRAM	Battery Backed Random Access Memory
CO	Crypto Officer
CU	Crypto User
CSP	Critical Security Parameter
CVL	Component Validation List
DAC	Device Authentication Certificate
DAK	Device Authentication Key
DH	Diffie Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm
EFP	Environment Failure Protection
EMI	Electro-Magnetic Interference
EMC	Electro-Magnetic Compatibility
FIPS	Federal Information Processing Standard
FSC	Firmware Signing Certificate
FSK	Firmware Signing Key

Term	Definition
GSK	Global Storage Key
HOC	Hardware Origin Certificate
HOK	Hardware Origin Key
HRNG	Hardware Random Number Generator
HSM	Hardware Security Module / Host Security Module
HMAC	Hash-based Message Authentication Code
ICD	Interface Control Document
I/O	Input / Output
IV	Initialization Vector
KAT	Known Answer Test
KBKDF	Key-Based Key Derivation Function
KCV	Key Cloning Vector
KDF	Key Derivation Function
KTS	Key Transport Scheme
LED	Light Emitting Diode
LSC	License Signing Certificate
LSK	License Signing Key
MAC	Message Authentication Code
MIC	Manufacturer’s Integrity Certificate
MIK	Manufacturer’s Integrity Key
MSK	Manufacturer’s Signature Key
NDRNG	Non-Deterministic Random Number Generator
OAEP	Optimal Asymmetric Encryption Padding
PEC	Password Encryption Certificate
PED	PIN Entry Device
PEK	Password Encryption Key

Term	Definition
PKCS	Public-Key Cryptography Standards
POST	Power-On Self Test
PSK	Partition Storage Key
PSO	Partition Security Officer
PU	Public User
RAM	Random Access Memory
RFC	Request For Comments
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMK	Security Officer’s Master Key
SP	Special Publication
STM	Secure Transport Mode
TUK3	Token Unwrapping Key 3
TWK3	Token Wrapping Key 3
TUK4	Token Unwrapping Key 4
TWK4	Token Wrapping Key 4
USB	Universal Serial Bus
USK	User's Storage Key

PREFACE

This document deals only with operations and capabilities of the Thales Luna Backup HSM Cryptographic Module in the technical terms of [FIPS 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.

REFERENCES

[FIPS 140-2] Federal Information Processing Standards Publication (FIPS PUB) 140-2, ‘Security Requirements for Cryptographic Modules’, May 25, 2001 (including change notices 12-02-2002).

[FIPS 140-2 IG] NIST, Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program, May 1, 2021.

[FIPS 180-4] Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS), NIST, August 2015.

[FIPS 186-4] Federal Information Processing Standards Publication 186-4, Digital Signature Standards (DSS), NIST, July 2013.

[FIPS 197] Federal Information Processing Standards Publication 197, Specification for the Advanced Encryption Standard (AES), November 26, 2001.

[FIPS 198-1] Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008.

[SP800-38A] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation – Methods and Techniques, December 2001.

[SP800-38F] NIST Special Publication 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012.

[SP800-56Ar3] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Revision 3, April 2018.

[SP800-56Br2] NIST Special Publication 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 2, March 2019.

[SP800-56Cr2] NIST Special Publication 800-56C, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, Revision 2, August 2020.

[SP800-90Ar1] NIST Special Publication SP800-90A, Recommendation for Random Number Generation Using Deterministic Bit Generators, Revision 1, June 2015.

[SP800-90B] NIST, SP800-90B, “Recommendation for the Entropy Sources Used for Random Bit Generation”, January 2018.

[SP800-108] NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009.

[SP800-131Ar2] NIST Special Publication 800-131A revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019.

[SP800-132] NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications, December 2010.

[SP800-133] NIST Special Publication 800-133 revision 2, Recommendation for Cryptographic Key Generation, June 2020

[PKCS #1] PKCS #1: RSA Cryptographic Standard, RSA Laboratories, v2.1.

1 Introduction

1.1 Purpose

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

1.2 Scope

This document applies to hardware versions 808-000064-005 and 808-000064-006 with firmware version 7.7.1 and bootloader version 1.3.0 or 1.5.0.

Both hardware parts are functionally equivalent with the difference being limited to supply choice for one of the non-security enforcing internal components.

The security policies described in this document apply to the Thales Luna Backup HSM Cryptographic Module only and do not include any security policy that may be enforced by the host appliance or server**.**

The security policies described in this document apply to the Cloning (CL) configurations with **PED and Password** authentication mechanisms of the Thales Luna Backup HSM Cryptographic Module.

The module is configured with support for both Password and PED based authentication by a license file loaded at the factory. The authentication type is selected by the operator during HSM initialization.

1.3 Validation Overview

The cryptographic module meets all level 3 requirements for FIPS 140-2 as summarized in the table below:

Table 1: FIPS 140-2 Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	3
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

Security Requirements Section	**Level**
Mitigation of Other Attacks	N/A

1.4 Functional Overview

The Thales Luna Backup HSM Cryptographic Module is a multi-chip standalone hardware cryptographic module in the small form factor device that connects to a computer workstation or server via USB. The cryptographic module is contained in its own enclosure that provides physical resistance to tampering.

The cryptographic boundary of the module is defined to encompass all components inside the secure enclosure.

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 outlined in section 3, ‘Guidance’ 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 USB communications interface. It also has a LCD touch screen for displaying system status.

A module provides secure key storage for symmetric keys and asymmetric key pairs and does not provide any symmetric and asymmetric cryptographic services other than transferring keys to and from the host HSM device. Access to key material 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 dedicated to the HSM Security Officer and Administrator role. Each partition must be separately authenticated in order to make it available for uses.

A SmartCard interface is present at the cryptographic module physical boundary but is unused in the certified configuration of the device as Thales Luna Backup HSM Cryptographic Module.

2 Module Overview

2.1 Module Specification

The cryptographic module is a multi-chip standalone hardware module in the small form factor device. The cryptographic boundary of the module is shown below:

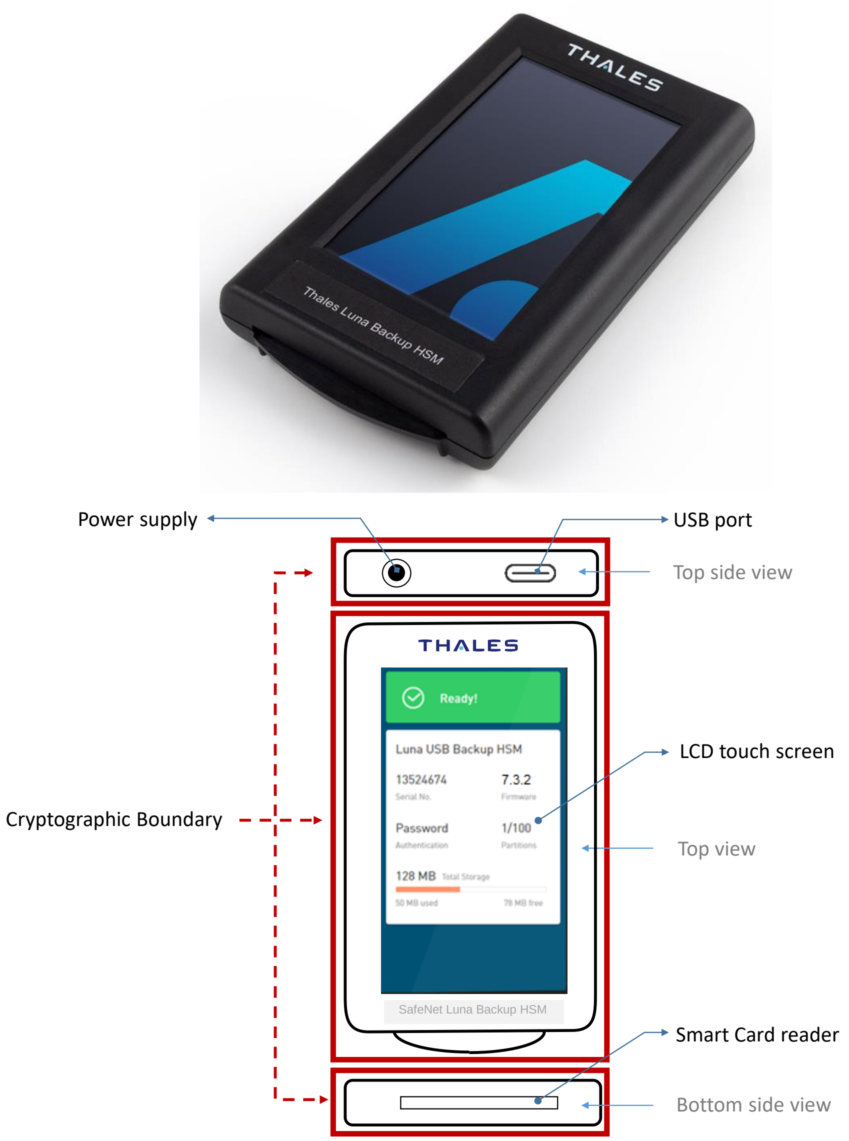

Figure 1: Thales Luna Backup HSM Cryptographic Module and cryptographic boundary

The cryptographic boundary is defined to encompass all components inside the enclosure, but excluding the following:

- LCD screen, ribbon cable and connector – this is currently only used to display status information;

- Internal Backup Battery – this is used to power the module real-time clock;
- SmartCard connector – this is un-used in the certified version of cryptographic module.

2.2 Ports and Interfaces

The module supports the following physical ports and interfaces:

- USB port
- LCD touch screen
- SmartCard reader
- Power supply

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

FIPS 140-2 Interface	Physical Interface	Logical Interface
Data Input	USB	Data I/O Luna ICD Logical Trusted Path (Luna PED – remote connection) Bootloader command protocol
	SmartCard reader	N/A - deactivated in certified firmware configuration and with the physical connector excluded from the cryptographic module boundary.
	LCD touch screen	Touch events
Data Output	USB	Data I/O Luna ICD Logical Trusted Path (Luna PED – remote connection) Bootloader command protocol
	SmartCard reader	N/A - deactivated in certified firmware configuration and with the physical connector excluded from the cryptographic module boundary.
Control Input	USB	Data I/O Luna ICD
Status Output	USB	Data I/O Luna ICD Logical Trusted Path (Luna PED – remote connection) Bootloader command protocol

FIPS 140-2 Interface	Physical Interface	Logical Interface
	LCD touch screen	System status
Power	5V - generated from an external 12V power supply module or USB port on the host machine	N/A
	3.6V battery	N/A

2.2.1 Trusted Path

If configured, the module can use a Thales Luna PED as the external data input/output devices. The Thales Luna PED connects to the module remotely over a secure network connection. The Thales Luna PED is used to pass authentication data and CSPs to and from the cryptographic module. In cases of the Luna PED, CSP's and authentication data are stored in an iKey connected to the Luna PED.

Any iKey, 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 iKey[1] are used with the Luna PED:

- Orange (RPV) Key – for the storage of the Remote PED Vector (RPV);
- Blue (Security Officer) Key – for the storage of HSM Security Officer, Partition Security Officer and Administrator authentication data[2];
- Black (Crypto Officer) Key – for the storage of Crypto Officer authentication data;
- Grey (Crypto User) Key – for the storage of Crypto User authentication data;
- Red (Cloning Domain) 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
- White (Auditor) Key – for the storage of Auditor authentication data.

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

[2] Separate iKey can be used when these roles are assigned to different operators

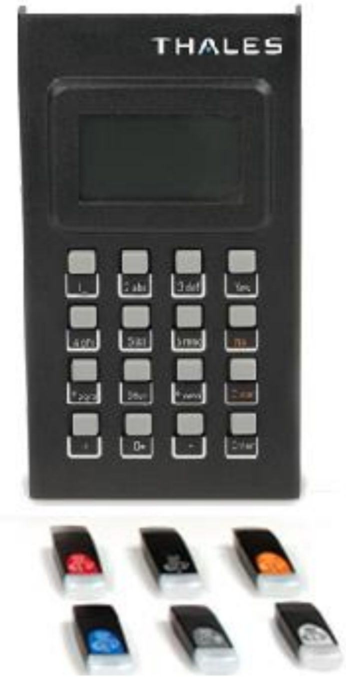

Figure 2: Thales Luna PED and iKey

When configured, the user connects the Thales Luna PED to a USB port on a management workstation. Remote PED operation use a secure protocol that authenticates both the Remote PED and the module and establishes an encrypted and authenticated communications channel between the module and the Remote PED.

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

- Thales Luna PED and cryptographic module will use the C(2e, 2s, ECC CDH) scheme from [SP800-56Ar3] 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 protects it using a HMAC-256 MAC. This is compliant with requirements from [SP800-38F] for key transport.

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.

2.2.2 SmartCard Reader

The Thales Luna Backup HSM Cryptographic Module does have a physical SmartCard reader to support a SmartCard authentication mechanism. The firmware configuration in this Security Policy does not activate the SmartCard authentication mechanism so the SmartCard reader is not used.

2.3 Roles and Services

2.3.1 Roles

The module supports the following roles:

Table 3: Thales Luna Backup HSM Cryptographic Module Roles

Role	Responsibilities
HSM Security Officer (HSM SO)	Module-level role. Initializes and configures the module for operation. Creates user partitions. Performs key management tasks for the admin partition. Performs cryptographic operations for the admin partition. Configures HSM level policies. Updates module firmware. Manages Administrator role[3].
Administrator	Optional admin partition-level Crypto Officer like role. Performs key management tasks for the admin partition. Performs cryptographic operations for the admin partition.
Auditor (AU)	Module-level role. Initializes, configures, and manages the secure audit logging feature.
Partition Security Officer (PSO)	User partition-level role. Configures container policies for user partition. Manages the CO Role[3].
Partition Crypto Officer (CO)	User partition-level role. Generates partition cryptographic keys for use by cryptographic services accessing the partition. Uses container keys[4] in order to support cryptographic services. Manages the CU Role[3].
Partition Crypto User (CU)	User partition-level role. Uses partition cryptographic keys.
Public User (PU)	Zeroizes HSM from local interfaces via command. Retrieval of status information. Collects module utilization statistics. Power cycle.

[3] Role is responsible for managing another role using the services (Initialize Role, Reset Role Authentication Data) defined in Table 5.

[4] Asymmetric Key Pairs (general partition) and Symmetric Keys (general partition).

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 Backup HSM Cryptographic Module	Role Scope
Crypto Officer	HSM Security Officer	Module
	Auditor	Module
	Partition Security Officer	User Partition
User	Administrator	Admin Partition
	Partition Crypto Officer	User Partition
	Partition Crypto User	User Partition
Unauthenticated User	Public User	Module/Partition

2.3.2 Services

All services listed in the table below can be accessed.

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

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 CU	Public User	Notes
HSM Factory Reset.	**Erased (for ALL partition):** PSK, USK, DRBG Internal State, KCV, SMK, Asymmetric Key Pairs (general partition), Symmetric Keys (general partition). In addition, the following HSM level keys are erased: SALK, CWK_{HSM}, CWK_{PED}, DEK_{HSM}, DMK_{HSM}, DEK_{PED}, DMK_{PED}.	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.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	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), Symmetric Keys (general partition). **Write:** DRBG Internal State, PEK, PEC, USK, PSK, KCV, Stored User Password Hash. **Used:** DRBG Internal State, PSK, USK, GSK, User Password, PED Authentication Data, Password.	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 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.	**Use:** DRBG Internal State. **Write:** DRBG Internal State, KCV.	x	-	-	-	-	-	-	None.
Delete a user partition.	**Erased (for partition instance of key object):** DRBG Internal State, PSK, USK, KCV, SMK, Asymmetric Key Pairs (general partition), Symmetric Keys (general partition).	x	-	-	-	-	-	-	Deleting a partition erases all partition object and roles.
Query HSM status.	None.	x	x	x	x	x	x	x	None.
Query partition status.	None.	x	x	x	x	x	x	x	None.
Query HSM configuration.	None.	x	x	x	x	x	x	x	None.
Query partition configuration.	None.	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 CU	Public User	Notes
Set HSM Level Policy (General).	**Erased (if destructive policy change requested):** For all partitions: DRBG Internal State, Asymmetric Key Pairs (general partition), Symmetric Keys (general partition), USK, PSK, KCV, SMK.	x	-	-	-	-	-	-	None.
Set Partition Level Policy (Admin Partition).	**Erased (if destructive policy change requested):** Asymmetric Key Pairs (general partition), Symmetric Keys (general partition), SMK.	x	-	-	-	-	-	-	None.
Set Partition Level Policy (User Partition).	**Erased (if destructive policy change requested):** Asymmetric Key Pairs (general partition), Symmetric Keys (general partition), SMK.	-	-	-	x	-	-	-	None.
Update Firmware.	**Used:** Root Certificate, Firmware Signing Certificate**.**	x	-	-	-	-	-	-	None.
Trigger HSM zeroization.	**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	Can be performed by any role. Equivalent to destroying the HSM through other means if physical access to the HSM is possible.
Trigger user partition zeroize.	**Erased:** USK, PSK, KCV, SMK, Asymmetric Key Pairs (general partition), Symmetric Keys (general partition).	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).

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition CU	Public User	Notes
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	None.
Submit external messages for entry into secure audit log.	**Used:** SALK, Secure Audit AppID-HMAC Key.	x	x	x	x	x	x	x	None.
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.
Clone SMK between Partitions.	**Use:** DRBG Internal State, Root Certificate, MIC, HOC, TWK3 and TWC3 (CPV1) and TUK4, TWK4 (CPV3), KEV_s (CPV1 only), KEV_t, KCV and Cloning Transfer Key. **Read/Write**: DRBG Internal State, SMK.	x	-	-	-	x	-	-	Used to underpin partition backup/restore operations to/from Luna Backup HSM. 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.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition CU	Public User	Notes
Clone partition objects between Partitions.	**Use:** DRBG Internal State, Root Certificate, MIC, HOC, TWK3 and TWC3 (CPV1) and TUK4, TWK4 (CPV3), KEV$_s$ (CPV1 only), KEV$_t$, KCV and Cloning Transfer Key. **Write:** DRBG Internal State, Asymmetric Key Pairs (general partition), Symmetric Keys (general partition).	x	x	-	-	x	x	-	Used to underpin partition backup/restore operations to/from Luna Backup HSM. Partition CU is able to clone public key objects only.
Store Partition Data Object.	None.	x	x	x	-	x	-	x	Used to underpin partition backup/restore operations to/from Luna Backup HSM. Used to store Scalable Key Storage (SKS) key blobs extracted from other HSM as data objects. When stored on Luna Backup HSM – the SKS key blobs are not decrypted and the HSM is used for external storage exclusively.
Read Partition Data Object.	None.	x	x	x	-	x	-	x	Used to underpin partition backup/restore operations to/from Luna Backup HSM.
Enable/disable STM.	**Use:** DRBG Internal State, STM Nonce. **Write:** DRBG Internal State.	x	x	x	x	x	x	x	Command can be executed un-authenticated if HSM is in zeroized state otherwise requires HSM SO role.
Request HSM self-test operation.	None.	x	x	x	x	x	x	x	None.
Query Role Status.	None.	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 CU	Public User	Notes
Initialize the Administrator.	**Use:** DRBG Internal State, USK, PSK, PEK. **Write:** DRBG Internal State, PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash.	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 AU.	**Use:** DRBG Internal State, USK, PSK, PEK. **Write:** DRBG Internal State, PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash.	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. 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 Internal State, USK, PSK, PEK. **Write:** DRBG Internal State, PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash.	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.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition CU	Public User	Notes
Initialize the Partition CO.	**Use:** DRBG Internal State, USK, PSK, PEK. **Write:** DRBG Internal State, PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash.	-	-	-	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 Internal State, USK, PSK, PEK. **Write:** DRBG Internal State, PEK, PEC, PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash.	-	-	-	-	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:** PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash. **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 CU	Public User	Notes
Change AU authentication data.	**Read:** USK **Use:** USK, PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash. **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:** PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash. **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:** PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash. **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 CU	Public User	Notes
Change authentication data for Partition CO / unlock role.	**Read:** USK **Use:** PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash. **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.
Change authentication data for Partition CU / unlock role.	**Read:** USK **Use:** PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash. **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.
Login to Access/Session as role.	**Use:** PEK (if password authentication used), PED Authentication Data, User Password (if challenge-secret enabled), Password, Stored User Password Hash. **Write:** recovered USK, PSK, KCV, GSK, SMK (if configured) (on successful presentation of correct login credentials).	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.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	Partition CU	Public User	Notes
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	`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.
Initialize Remote PED Vector (RPV).	**Use:** GSK. **Write:** RPV, RPV-C, RPV-K, PED-SKA-C and PED-SKA-K.	x	-	-	-	-	-	-	None.
Setup Remote PED Session.	**Use:** ECC MIC, ECC-HOC$_{PED}$, PAC, RPV-C, PED-SKA-C, PED-EKA-C, HSM-EKA-C, HSM-EKA-K, HSM-EKA-C, PED Master Shared Secret, DEK$_{HSM}$, DEK$_{PED}$, DMK$_{HSM}$, CWK$_{HSM}$, CWK$_{PED}$. **W:** DEK$_{HSM}$, DEK$_{PED}$, DMK$_{HSM}$, CWK$_{HSM}$, CWK$_{PED}$.	x	x	x	x	x	x	x	This service is used to derive a number of shared keys between the module and a remote Thales Luna PED.
Read non-sensitive key attribute where `CKA_PRIVATE = false` for a given key object.	None.	x	x	x	x	x	x	x	Only possible for partition objects cloned into the Backup HSM using CPV1 or CPV3. This is not possible for objects backed up as encrypted blobs where these were extracted from other HSM using SKS but are stored as data objects on Luna backup HSM.

Service	Cryptographic Keys and CSPs (Used, Create, Read, Write or Erased)	HSM SO	Administrator	AU	Partition SO	Partition CO	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	Only possible for partition objects cloned into the Backup HSM using CPV1 or CPV3. This is not possible for objects backed up as encrypted blobs where these were extracted from other HSM using SKS but are stored as data objects on Luna backup HSM.
Re-seed partition random number generator (RNG).	**Use:** DRBG Seed, DRBG Internal State. **Write**: DRBG Seed, DRBG Internal State.	x	x	x	x	x	x	x	None.
Request complete erase of the HSM firmware image and key stores (excludes erase of bootloader).	**Erase:** Results in the complete erase of all module CSP with the exception of the Root Certificate.	x	x	x	x	x	x	x	Only used to recover from corrupt firmware as performed as a factory operation. 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	Includes the hardware part number.
Request authentication and execution of main firmware.	**Use:** Root Certificate and Firmware Signing Certificate.	x	x	x	x	x	x	x	None.

2.4 Authentication

All roles except for the Public User must authenticate to the module by providing their authentication data.

Table 6: Roles and Required Identification and Authentication and Table 7: Strengths of Authentication Mechanisms, explain the type and strength of the authentication data supported for each role.

If configured to use the Thales Luna PED for authentication, all roles must authenticate using an iKey and where, when a role is initialized, a module generates the authentication data as a 48-byte random value and writes it to the iKey. Optionally, the Crypto-Officer and Crypto-User roles can be configured to use two-factor authentication by in additional 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 [SP800-56Br2].

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 (iKey)
Auditor	Identity-based	Password	Authentication token (iKey)
Partition Security Officer	Identity-based	Password	Authentication token (iKey)
Crypto Officer	Identity-based	Password	Authentication token (iKey), plus optional password
Crypto User	Identity-based	Password	Authentication token (iKey), plus optional password
Administrator	Identity-based	Password	Authentication token (iKey)
Public User	Not Required	N/A	N/A

Table 7: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
PED Key	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}. With a maximum of 6000 failed login attempts per minute[5], the thresholds required by [FIPS 140-2] can never be reached ($1.52e^{-112}$).
Password	User provided byte array (minimum 7 bytes). The probability of guessing the challenge secret in a single attempt is 1 in 2^{56}. With a maximum of 6000 failed login attempts per minute[5], the thresholds required by [FIPS 140-2] can never be reached ($8.33e^{-14}$).

When using the password authentication mechanism, the module encrypts a known check-word under a key derived using PBKDF from [SP800-132] 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 check-word. Successful login is achieved if the decrypted check-word 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)[6].

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

[5] This is based on testing and the bandwidth limitation of authentication (e.g., 100 attempts per second, or 6000 attempts per minute). So, it represents an actual result of testing.

[6] When 'decommission' is enabled as a module capability, the USK is independently encrypted in storage under USK which is independently also encrypted under the module generated KEK.

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 [SP800-132] 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.

2.4.1 Activation

If PED authentication is configured, the 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[7].

2.4.2 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 Thales Luna PED in order to reconstruct the original secret.

2.5 Physical Security

The Thales Luna Backup HSM Cryptographic Module is a multi-chip standalone module as defined by [FIPS 140-2], section 4.5.

The whole module enclosed in a plastic casing 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 plastic 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 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 the power on state.

In the event that the module senses an out-of-range temperature or over voltage, the module will reset itself, clear all working memory and log the event.

[7] A module is reset in response to EFP violations, loss of power or a request from a host application.

2.5.2 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 SHA2-256 digest of the random string, module CSPs, firmware, module configuration information and non-volatile memory.

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 module 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.

2.5.3 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[8] 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.

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:

[8] 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.

Table 8: FIPS-Approved Algorithm Implementation

CAVP Cert	Algorithm and Standard	Mode / Method /Strength	Use / Function
Symmetric Encryption/Decryption			
C2020	**Algorithm:** AES **Standards:** [FIPS 197], [SP800-38A] and [SP800-38F].	**Mode:** CBC, KWP. Key Size: 256-bits.	Used to support the following services: > Initializing authentication data and roles (Initialize the HSM, Initialize the Administrator, Initialize the AU, Initialize the Partition SO, Initialize the Partition CO, Initialize the Partition CU); > Changing authentication data for roles (Change HSM SO authentication data, Change authentication data for Administrator / unlock role, Change AU authentication data, Change Partition SO authentication data, Change authentication data for Partition CO / unlock role, Change authentication data for Partition CU / unlock role); > Key Retrieval and Storage (all services using CSP listed in Table 5: Roles and Access Rights by Service). > Cloning Operations (Clone partition objects between Partitions and Clone SMK between Partitions); > Export/import audit log secret key; and > Login to Access/Session as role.

CAVP Cert	Algorithm and Standard	Mode / Method /Strength	Use / Function
Hashing			
C2020	**Algorithm:** SHA **Standards:** [FIPS 186-4].	**Methods:** SHA1, SHA2-256, SHA2-384, SHA2-512.	Used to support the following services: > Cloning operations (Clone SMK between Partitions and Clone partition objects between Partitions) - signatures and object integrity. > Create a user partition; > Load Configuration Update File; > Login to Access/Session as role; > Setup Remote PED Session; > Request HSM self-test operation; > Update Firmware; > Submit external messages for entry into secure audit log; > Validate the audit log; and > Read non-sensitive key attribute where CKA_PRIVATE = true for a given key object (this is the only service using SHA1 where it's used to generate the output when reading the legacy object attribute CKA_ FINGERPRINT_SHA1).
C2022	**Algorithm:** SHA **Standards:** [FIPS 186-4].	**Methods:** SHA1, SHA2-256, SHA2-384 (Byte Only).	Used to support the following services: > Request authentication and execution of main firmware.
Message Authentication Code			
C2020	**Algorithm:** HMAC **Standard:** [FIPS 198-1].	**Methods:** HMAC-SHA2-256, HMAC-SHA2-512.	Used to support the following services: > Submit external messages for entry into secure audit log; > Validate the audit log; and > Setup Remote PED Session.

CAVP Cert	Algorithm and Standard	Mode / Method /Strength	Use / Function
Asymmetric			
C2020, C2021	**Algorithm:** RSA **Standard:** [FIPS 186-4].	**Methods:** Key Generation. **Modulus length:** 2048-bit. **Generation Method:** B.3.6.	Used to support the following services: > Clone partition objects between Partitions (when using CPV1 – import only) – generated keys are used with the RSA CVL to encrypt the KEVt and KEVs used during CPV1.

A674, A675	**Algorithm:** RSA
	Standard: [FIPS 186-4].
		Methods: Key Generation, Signature Generation, Signature Verification.
		Modulus length: 4096-bit.
		Signature Type: PKCS#1 v1.5.
		Generation Method: B.3.6.
		Hash: SHA2-384, SHA2-512.
			Used to support the following services:
			> Clone partition objects between Partitions (when using CPV3);
			> Clone SMK between Partitions (when using CPV3);
			> Update Firmware;
			> Load Configuration Update File;
			> Request HSM self-test operation.

C2022	**Algorithm:** RSA **Standard:** [FIPS 186-4].	**Methods:** Signature Verification. **Modulus Length:** 4096-bits **Signature Type:** PKCS#1 v1.5. **Hash:** SHA2-384.	Used to support the following services: > Request authentication and execution of main firmware.
C2020	**Algorithm:** ECDSA **Standard:** [FIPS 186-4].	**Methods:** Key Generation, Signature Generation, Signature Verification. **Curves:** P-521.	Used to support the following services: > Setup Remote PED Session.
C2020, C2021	**Algorithm:** RSA (CVL) **Standards:** [PKCS #1], section 5.1.2.	**Methods:** Decryption Primitive.	Used to support the following services: > Clone partition objects between Partitions (CPV1 – import only).
Key Agreement Scheme			
A2125	**Algorithm:** KAS. **Standards:** [SP800-56Ar3] and [SP800-56Cr2].	**Scheme:** Full Unified Model C(2e, 2s, ECC CDH) **Methods:** Full Validation, Key Pair Generation. **Supported curves:** P-521. **KDF methods:** One Step, Supported hash: SHA2-512. **Key confirmation:** HMAC-SHA2-512 with 256-bit key.	Used to support the following services: > Setup Remote PED Session.

CAVP Cert	Algorithm and Standard	Mode / Method /Strength	Use / Function
A2125	Algorithm: KAS-RSA Standards: [SP800-56Br2] and [SP800-56Cr2].	**Method**: KAS1-Basic. Modulus length - 4096 bits, key generation method – rsakpg1-prime-factor, KDF method – One-Step Key Derivation from SP800-56Cr2 using SHA2-512, fixed public exponent – 65537. Caveat: Cert. #A2125; key establishment methodology provides 150 bits of encryption strength	Used to support the following services: > Clone partition objects between Partitions (CPV3); and > Clone SMK between Partitions (CPV3).
Key Transport			
C2020	**Algorithm:** KTS (AES Certs. #C2020) **Standards:** [FIPS 197] and [SP800-38F].	**Modes:** KWP. **Key size:** 256-bits.	Used to support the following services: > Clone partition objects between Partitions (CPV3); > Clone SMK between Partitions (CPV3); > Setup Remote PED Session.
A2125	**Algorithm:** KTS-RSA **Standards:** [SP800-56Br2].	**Method:** KTS-OAEP-Basic **Modulus Length**: 4096. **Hash:** SHA2-512. **Key Length:** 256. Caveat: Cert. #A2125; key establishment methodology provides 150 bits of encryption strength	Used to support the following services: > Login to Access/Session as role – used to decrypt password using the PEC protocol.
Key Derivation Function			
C2020	**Algorithm:** Key-Based Key Derivation Function (KBKDF) **Standards:** [SP800-108]	Key-Based Key Derivation Function (KBKDF) KDF Mode: Counter. MAC Mode: HMAC-SHA2-512.	Used to support the following services: > Login to Access/Session as role – used to derive the USK encryption key used to decrypt the USK and known check-word during authentication attempts when module configured for PED authentication.

CAVP Cert	Algorithm and Standard	Mode / Method /Strength	Use / Function
A2125	**Algorithm:** KDA **Standards:** [SP800-56Cr2]	KDA (Cert. #A2125) One-Step Key Derivation using SHA2-512.	Used to support the following services: > Clone partition objects between Partitions (CPV3); > Clone SMK between Partitions (CPV3); > Setup Remote PED Session; and > Clone partition objects between Partitions (CPV1 – import only).
A2125	**Algorithm:** PBKDF[9] **Standards:** [SP800-132]	**Methods:** SHA2-512 **Derived Key Length:** 256-bits **Password Length:** 128-bits **Salt Length:** 256-bits	Used to support the following services: > Login to Access/Session as role – used to derive the known check-word used to validate authentication attempts when module configured for password authentication.

[9] Used internal to the cryptographic module to derive the storage encryption key used to encrypt the check-word 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 [SP800-132] where the derived Master Key (MK) is used directly as the Data Protection Key (DPK).

CAVP Cert	Algorithm and Standard	Mode / Method /Strength	Use / Function
Random Number Generation			
C2020	**Algorithm:** HASH_DRBG **Standard:** [SP800-90Ar1]	**Mode:** SHA2-256. **Security strength:** 256-bits	Used to support the following services that consume entropy: > Initializing services when using PED authentication (Initialize the HSM, Initialize the Administrator, Initialize the AU, Initialize the Partition SO, Initialize the Partition CO, Initialize the Partition CU); > Changing authentication data for PED authenticated roles (Change HSM SO authentication data, Change authentication data for Administrator / unlock role, Change AU authentication data, Change Partition SO authentication data, Change authentication data for Partition CO / unlock role, Change authentication data for Partition CU / unlock role); > Generating keys during cloning (Clone partition objects between Partitions and Clone SMK between Partitions); > Setup Remote PED Session; > Create a user partition; > Enable/disable STM (used to generate the STM Nonce when enabling STM); and > Re-seed partition random number generator.

CAVP Cert	Algorithm and Standard	Mode / Method /Strength	Use / Function
Vendor affirmed, using [FIPS 140-2 IG], D.12.	**Algorithm:** CKG **Standard:** [SP800-133]	CKG[10]	Used to support the following services that generate keys: > Initialize the HSM; > Generating keys during cloning (Clone partition objects between Partitions and Clone SMK between Partitions); > Setup Remote PED Session; and > Create a user partition.

Table 9: Allowed Security Function for the Firmware Implementation

Allowed Security Functions	Use / Function
Key Transport	
AES (key unwrapping; key establishment methodology provides 256 bits of encryption strength) (based on AES Cert. #C2020 and using allowances in [FIPS 140-2 IG], D.9).	Used to support the following services: > Clone partition objects between Partitions (CPV1 – import only).
RSA (CVL Certs. #C2020 and #C2021, key unwrapping; key establishment methodology provides between 112 and 150 bits of encryption strength)[11] Modulus length – 2048.	Used to support the following services: > Clone partition objects between Partitions (CPV1 – import only).
NDRNG	Used to support the following services: > Internal service used to generate the seed used to instantiate the module DRBG; and > Re-seed partition random number generator.

[10] Symmetric keys and seeds used for asymmetric key generation are an unmodified output from the approved DRBG (Cert. #C2020)

[11] Only permitted for use under [FIPS 140-2 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.

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, ‘Guidance’ for further details on configuring the approved mode of operation).

> **Symmetric Encryption/Decryption**

- DES
- Triple-DES
- 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
- 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)

> **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
Root Certificate	RSA-4096 public key certificate	N/A – generated outside the module.	Certificate output in plaintext. Loading during manufacture as part of the module bootloader.	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	N/A – generated outside the module.	N/A - Stored outside the module on Thales managed "Root" HSM	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	N/A – generated outside the module.	N/A - Stored outside the module on Thales managed "Root" HSM	The subordinate root signing key used to certify HSM firmware updates.
Firmware Signing Certificate	RSA-4096 public key certificate	N/A – generated outside the module.	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.
License Signing Key	RSA-4096 private key	N/A – generated outside the module.	N/A - Stored outside the module on Thales managed "Root" HSM	The subordinate root signing key used to certify HSM capability updates.
License Signing Certificate	RSA-4096 public key certificate	N/A – generated outside the module.	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 during manufacture.	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	N/A – generated outside the module.	N/A - Stored outside the module on Thales managed "Root" HSM	The subordinate root signing key used to certify HSM 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 during manufacture.	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.
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 (KEV_s and KEV_t) 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 (KEV_s and KEV_t) as part of the handshake during the cloning protocol.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Cloning Key Encryption Vector – source (KEV_s)	384 bit nonce.	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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.	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	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.
Token or Module Variable Key (TVK)	AES-256	[SP800-90Ar1] HASH_DRBG using SHA2-256.	Not Input or Output.	It is used to encrypt authentication data stored for auto-activation purposes.
STM Nonce	992-bit random number	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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 Seed	384 bits	Output from Hardware Noise Source (NDRNG).	Not Input or Output.	Random seed data drawn from the Hardware RBG and used to seed an implementation of the HASH_DRBG [SP800-90Ar1]. Seed is zeroized immediately following use.
DRBG Internal State (V, C and reseed counter)	Hash-DRBG State	Stored from Initialize operation of DRBG.	Not Input or Output.	Secret state of the approved DRBG. The value is generated using the methods described in [SP800-90Ar1] for DRBG Instantiation and using the DRBG Seed taken from internal hardware noise source.
Global Storage Key (GSK)	AES-256	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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).	[SP800-90Ar1] HASH_DRBG using SHA2-256 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-KWP 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 Auditor 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	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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 SP800-56Br2.	User provided password input by the operator as a second factor of authentication data.
PED Authentication Data (if PED configuration)	48-byte random value	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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 Thales Luna 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 SP800-56Br2.	User provided password input by the operator as authentication data.
Stored User Password Hash	256-bits	[FIPS 186-4] SHA2-512	Not Input or Output.	Hashed user password with 256-bit random salt. CSP is compared with salted hash of passwords supplied by the end-user as part of login when using PED authentication with optional memorized secret.
User Storage Key (USK)	AES-256	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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.
USK encryption key	AES-256	PBKDF [SP800-132] when module is configured for Password based authentication. KBKDF [SP800-108] when module is configured for PED authentication.	Not Input or Output.	Recovered during login attempts to the module and used to decrypt (AES-256 in KWP mode) a known check-word used during authentication attempts alongside the USK. Derivation method for the key varies depending on the authentication method configured for the module.
Key Cloning Domain Vector (KCV)	48-byte random value (PED configuration) Or 7 - 255 character data string (Password configuration).	[SP800-90Ar1] HASH_DRBG using SHA2-256 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	[SP800-90Ar1] HASH_DRBG using SHA2-256.	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 certificate with 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 Thales Luna PED.
HSM Static Key-Agreement Certificate for Remote Connections (HSM-SKA-C$_{REMOTE}$)	ECC public key certificate with 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.
HSM Ephemeral Key-Agreement Certificate (HSM-EKA-C)	ECC public key certificate with 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 Thales 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 certificate with 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 certificate with 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 Thales Luna PED's ECC ephemeral public key for C(2e,2s, 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.
PED Master Shared Secret	256-bit	ECDH from [SP800-56Ar3] and using C(2e,2s, ECC CDH) with curve P-521.	Not Input or Output.	Intermediate key value used during setup of the Local and Remote PED channel. Key is the output of the ECDH function and used to generate HSM and PED CSP Wrapping Key, MAC key, IV and Data Encryption Key. Keys are generated using OneStep KDF from [SP800-56Cr2] with SHA2-512.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
HSM CSP Wrapping Key (CWK$_{HSM}$)	AES-256	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	Not Input or Output.	Derived during Local and Remote PED Channel for wrapping exchanged CSPs.
PED CSP Wrapping Key CWK$_{PED}$	AES-256	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	Not Input or Output.	Derived during Local and Remote PED Channel for wrapping exchanged CSPs.
HSM Data Encryption Key (DEK$_{HSM}$)	AES-256	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	Not Input or Output.	Derived during Remote PED Channel for encrypting communication messages (from HSM-to-PED).
HSM MAC Key (DMK$_{HSM}$)	256 bits	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	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	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	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	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	Not Input or Output.	Derived during Remote PED Channel for encrypting communication messages (from PED-to-HSM).
PED MAC Key (DMK$_{PED}$)	256 bits	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	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	OneStep KDF from [SP800-56Cr2] and using SHA2-512 [FIPS 180-4] as the PRF.	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.

Keys and CSPS	CSP Type	Generation	Input / Output	Description
Asymmetric Key Pairs (general partition)	RSA, DSA, ECC, DH	N/A	When imported using CPV1– encrypted under the Cloning Transfer Key. When imported/exported using CPV3 – encrypted under the Cloning Transfer Key. Refer to Section 2.8.2 for additional details.	Asymmetric key pairs that can be exported/imported from/to the module for storage. Keys cannot be used whilst stored on the cryptographic module.
Symmetric Keys (general partition)	AES or Triple-DES, MAC, KDF.	N/A	When imported using CPV1– encrypted under the Cloning Transfer Key. When imported/exported using CPV3 – encrypted under the Cloning Transfer Key. Refer to Section 2.8.2 for additional details.	Symmetric keys that can be exported/imported from/to the module for storage. Keys cannot be used whilst stored on the cryptographic module.

2.8.1 Key Generation

Symmetric cryptographic keys are generated by the direct unmodified output of the module's 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 and MIC.

The HOC is 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 DRBG (Hash-DRBG using SHA2-256) [SP800-90Ar1] is seeded using 384-bits or raw entropy taken from the module NDRNG. Based on calculated min-entropy values (H=0.943429) for the platform raw noise source and factors outlined in [SP800-90B], the 384-bit input used to seed the DRBG is considered to have 362-bits of entropy.

2.8.2 Key Import and Export

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

> Physical Trusted Path (remote 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: Summary of CSPs.

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 [SP800-56Br2] 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 [SP800-56Cr2] 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.

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

CPV1 is supported to enable the import/export of keys from existing Thales HSM with firmware version 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 SP800-56Cr2 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.

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 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
SHA KAT (SHA1, SHA2-256, SHA2-384).	Power-on	Error output and module halt
RSA KAT (Signature Verification)	Power-on	Error output and module halt
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[12]	Error output and module halt

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)	Power-on	Error output and module halt
SHA KAT (SHA1, SHA2-256, SHA2-384, SHA2-512).	Power-on/Request	Error output and module halt
HMAC KAT (HMAC-SHA2-256, HMAC-SHA2-512).	Power-on/Request	Error output and module halt
RSA KAT (Signature Generation, Signature Verification)	Power-on/Request	Error output and module halt

[12] Request indicates triggering a POST via a command

Test	When Performed	Indicator
AES KAT (CBC and KWP modes) covering 256 bit keys. Encrypt and decrypt operation performed for each mode.	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.
KDF KAT (Derive using HMAC-SHA2-512 as PRF).	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[13]	Continuous	Firmware / Hardware	Error output and module halt
RSA – 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

[13] 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 140-2 IG], 9.8 for modules implementing an approved DRBG from [SP800-90Ar1].

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, ‘Scope’. The following sections provide guidance on checking each element.

Any module displaying 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 validation.

In order to check the bootloader, hardware and firmware version the LunaCM[14] client tool is used with the **`hsm showinfo`** command.

Expected output from the command with example bootloader, hardware and firmware versions highlighted for convenience in red is shown below:

```
lunacm:>hsm showinfo

            Slot Id -> 108
            Partition Label -> myG7Pwd
            Partition Serial Number -> 132525
            Partition Model -> Luna G7
            Partition Manufacturer -> Safenet, Inc.
            Partition Status -> L3 Device, OK
            Session State -> CKS_RW_PUBLIC_SESSION
            Role Status ->   none logged in
            RPV Initialized -> No

            Partition Cloning Version -> 1
            Partition FM Status -> FM Disabled

            Partition SMK OUIDs:
                        SMK-FW4: Not Initialized
                        SMK-FW6: Not Initialized
                        SMK-FW7-FM: Not Initialized
                        SMK-FW7-Rollover: Not Initialized
                        SMK-FW7-Primary: Not Initialized


            Partition Storage:
                        Total Storage Space:  655360
                        Used Storage Space:   0
                        Free Storage Space:   655360
                        Object Count:         0
                        Overhead:             24224

            HSM Storage:
                        Total Storage Space:  33816576
```

[14] LunaCM maps to the Luna ICD logical interface at the cryptographic module boundary.

```
                        Used Storage Space:   962968
                        Free Storage Space:   32853608
                        Allowed Partitions:   100
                        Number of Partitions: 3

            HSM Part Number -> 808-000064-005

            Environmental:
                        System Temperature :  46 deg. C
            Firmware Version -> 7.7.1
            Bootloader Version ->  1.3.0
            Rollback Firmware Version -> 7.3.2

            License Count:
                        1. 621000121-000 G7 BU 32M Base CUF December 7 2018

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

Command Result : No Error
```

Figure 3: Example output of `hsm show` command from LunaCM.

To be in a FIPS compliant mode of operation, the versions output by the tool must correspond to the hardware identifier options, bootloader and firmware versions covered in section 1.2, ‘Scope’.

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 (55), “Enable Restricted Restore”** – this is disabled by default and shall be enabled.

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 this policy is left (or put) in the “disabled” 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 line highlighted in green on Figure 3.

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 the Approved mode of operation, any changes to HSM Policy (55) (going from Approved to non-Approved mode) will trigger an automatic zeroization of the HSM erasing all roles and partition stored key objects.