THALES

Luna T7 Cryptographic Module

FIPS 140-2 Level 3 Security Policy - Non-Proprietary

002-500015-001
Revision H
09 April 2021

DOCUMENT CHANGE HISTORY

Revision	Date	Author	Reason for Change	Sections Affected
A	2020-05-01	MFW	First issue of document, incorporated internal review comments	All
B	2020-07-15	MFW	Incorporate updates from firmware changes and source code review.	All
C	2020-07-27	MFW	Incorporate more comments from Security Policy review.	All
D	2020-07-30	MFW	Update based on final review comments.	All
E	2021-02-17	MFW	Update based on NIST Coordination comments.	All
F	2021-03-02	MFW	2nd update based on NIST and evaluator comments.	All
G	2021-04-07	MFW	Integrated 3rd round of NIST comments. Removed r2 from Vendor Affirmation of SP800-56B.	2.7.1
H	2021-04-09	SML	Update based on round 4 NIST comment. Changed KDF entry in Table 2-6 to KDA to match certificate entry.	Table 2-6

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Purpose

This non-proprietary document describes the security policies enforced by Thales Trusted Cyber Technologies' Luna T7 Cryptographic Module.

The Luna T7 Cryptographic Module can be used as follows:

- A standalone device called the Luna PCIe HSM (T-Series)
  https://www.thalestct.com/luna-PCIe-hsm
- An embedded device in the Luna Network HSM (T-Series)
  https://www.thalestct.com/luna-network-hsm
- An embedded device in the CipherTrust Manager
  https://www.thalestct.com/ciphertrust-manager

This document applies to Luna T7 Cryptographic Module Hardware Versions 872-500024-001 and 872-500025-001 with Firmware Version 7.11.1 and Boot Loader Version 2.0.1.

1.2 Scope

The security policies described in this document apply to the Luna T7 Cryptographic Module only and do not include any security policy that may be enforced by the host appliance or server.

The policy of the Luna T7 Cryptographic Module can be configured for either Password or PED based authentication. The default setting is Password based authentication. The Security Officer (SO) can change the authentication mode between Password and PED. The configuration of the module can be verified by the operator by issuing a 'show policy' command.

1.3 Validation Overview

The cryptographic module meets all level 3 requirements for FIPS 140-2 as summarized in Table 1-1.

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
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

TABLE 1-1: FIPS 140-2 SECURITY LEVELS

1.4 Functional Overview

The Luna T7 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 Boundary of the 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. Figure 2-1 depicts the Luna T7 Cryptographic Module and highlights the Cryptographic Boundary, Figure 2-2 shows the ports on the PCI bracket, and Figure 2-3 depicts the Luna Network HSM T-Series appliance with the Luna T7 Cryptographic Module installed and the PED and PED Keys which can be used for authentication.

A module may be explicitly configured to operate in either FIPS 140-2 Approved mode, or in a Non-Approved mode of operation. Note that selection of operating in FIPS 140-2 Approved mode occurs at initialization of the Cryptographic Module, and cannot be changed during normal operation without zeroizing the module's non-volatile memory. Section 3.1 provides additional information for configuring the module in FIPS 140-2 Approved mode of operation.

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

A module provides secure key generation and storage for symmetric keys and asymmetric key pairs along with symmetric and asymmetric 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 definitions or "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 role. Each partition must be separately authenticated in order to make it available for use.

2. Module Overview

2.1 Module Specification

The Luna T7 Cryptographic Module is a multi-chip embedded hardware module which is available by itself as a Luna PCIe HSM T-Series device, embedded within a Luna Network HSM T-Series appliance, or embedded within a CipherTrust Manager. The Cryptographic Boundary of the module is shown in red in Figure 2-1.

872-500024-001 is the base Luna T7 PCIe Hardware Module shown in Figure 2-1. The 872-500025-001 Hardware Module is identical to the 872-500024-001, except that the 872-500025-001 has additional components within the Cryptographic Boundary to support an additional, quantum entropy source, as outlined in Table 2-9.

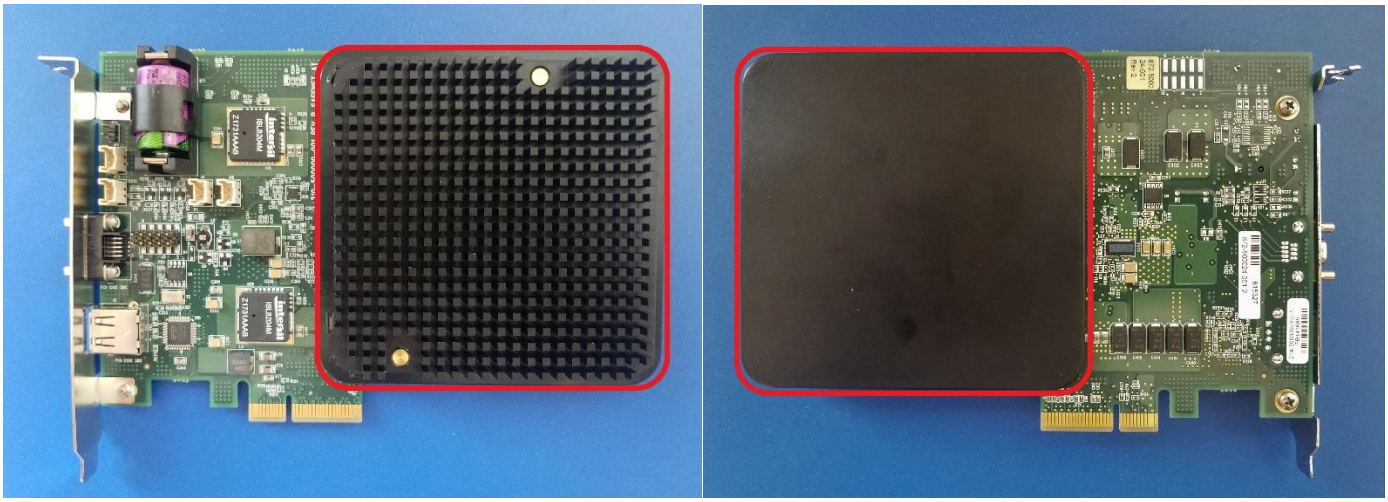

FIGURE 2-1: LUNA T7 CRYPTOGRAPHIC MODULE, TOP AND BOTTOM VIEWS, WITH CRYPTOGRAPHIC BOUNDARY IN RED

The Physical Ports on the PCI Bracket are shown in Figure 2-2. Port 1 is the Micro-DB9 for the Serial PED cable and Port 2 is the Type A USB 2.0 port for the Backup HSM.

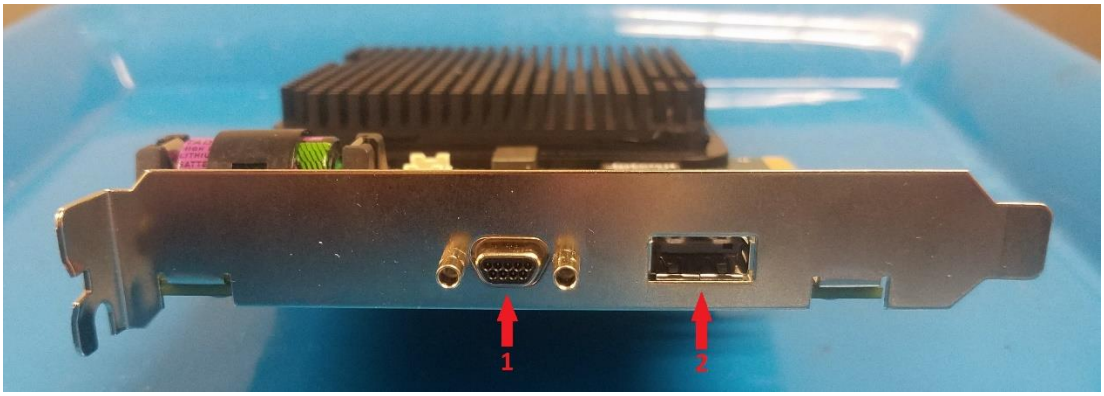

FIGURE 2-2: LUNA T7 CRYPTOGRAPHIC MODULE, PCI BRACKET VIEW

Figure 2-3 shows a Luna Network HSM (T-Series), one of the embedments for the Luna T7 Cryptographic Module, and an external PED device and PED Keys.

FIGURE 2-3: LUNA NETWORK HSM T-SERIES (WITH T7 INSTALLED), PED AND PED KEYS

2.2 Ports and Interfaces

The module supports the following physical ports and interfaces:

- PCIe interface
- Serial PED
- USB Host
- Power supply
- Battery
- LED
- External event input
- Decommission input

FIPS 140-2 Interface	Physical Interface	Logical Interface
Data Input	PCIe interface	Data I/O Luna ICD Logical Trusted Path (Remote PED) Bootloader command protocol
	Serial PED	Physical Trusted Path (Local PED)
	USB Host	Physical Trusted Path (Backup HSM)
Data Output	PCIe interface	Data I/O Luna ICD Logical Trusted Path (Remote PED) Bootloader command protocol
	Serial PED	Physical Trusted Path (Local PED)
	USB Host	Physical Trusted Path (Backup HSM)
Control Input	PCIe interface	Data I/O Luna ICD
	External event jumper	N/A
	Decommission jumper	N/A
Status Output	PCIe interface	Data I/O Luna ICE Logical Trusted Path (Remote PED) Bootloader command protocol
	Serial PED	Physical Trusted Path (Local PED)
	USB Host	Physical Trusted Path (Backup HSM)
	LED	N/A
Power	12V 5V, 3.3V, 1.5V, 1.35V, 1V (generated from PCIe 12V supply)	N/A
	3.6V (battery)	N/A

TABLE 2-1: MAPPING OF FIPS 140-2 INTERFACES TO PHYSICAL AND LOGICAL INTERFACES

2.2.1 Trusted Path – Backup HSM

If configured, the Luna T7 Cryptographic Module can copy keys, user data, or module data to a Backup HSM that is connected to the Type A USB Host port on the T7. The T7 operates as the USB Host (Root Hub) port and the Backup HSM operates as the USB Device on this interface.

It is also possible to clone Luna T7 user objects to remote HSMs across the standard PCIe command and data I/O interface. In both cases, whether the Backup HSM is remote or connected to the module's USB Host port, the cloning operation is initiated and controlled by the PCIe Host. The PCIe Host issues the commands to initialize the Source and the Target HSM and ensure the secure agreement of the session key that is used to encapsulate the objects passed from the Source to the Target.

The Luna T7 Cryptographic Module firmware has been built so that the only driver loaded for the USB Host port is for the Backup HSM. Also, the USB Host driver utilizes a whitelist that will only enumerate a Backup HSM as a USB Device.

2.2.2 Trusted Path – Local PED

If configured, the Luna T7 Cryptographic Module can use a Luna PED as an external data input/output device. The Luna PED connects to the module's Serial PED port and is used to pass authentication data and CSPs to and from the module via a physical trusted path. CSPs 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 are used with the Luna PED:

- Orange (RPV) PED Key – for the storage of the Remote PED Vector (RPV)
- Blue (SO) PED Key – for the storage of Security Officer and Administrator authentication data
- Black (User) PED Key – for the storage of User authentication data
- Red (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
- Purple (MTK Recovery) PED Key – for the storage of an external split that allows the MTK to be recovered after a tamper event
- White (Audit Officer) PED Key – for the storage of Audit Officer authentication data

2.2.3 Remote PED

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 protocol over the PCIe interface that authenticates both the remote PED and the module and establishes a one-time AES-256-CBC/HMAC-SHA-256 key to encrypt the communications 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 module and the Remote PED is secured in the manner described below.

At the time the Luna PED is configured for remote use, the module generates a random 256-bit secret, known as the Remote PED Vector (RPV), stores it in its internal parameters area, and writes it to the "Orange" PED Key, also known as the Remote PED Key (RPK), using a locally attached Luna PED.

To establish the secure connection, the RPK must be inserted into the Luna PED connected to a management workstation. The PED extracts the RPV, and the PED and the cryptographic module then participate in an ephemeral Elliptic Curve Diffie-Hellman (ECC CDH) key agreement session as specified for the Ephemeral Unified Model in SP800-56Ar3. The shared secret is then used in a Two-Step Key Derivation Function with Randomness Extraction per SP800-56Cr1 and SP800-108, with the preshared RPV as OtherInfo to produce the key to be used for the session. An exchange of encrypted random nonces is performed to authenticate both ends of the transmission. All traffic between the PED and the cryptographic module is encrypted and authenticated in the session tunnel using AES-256-CBC and HMAC-SHA-256.

2.3 Roles and Services

2.3.1 Roles

The Luna T7 Cryptographic Module supports the following authenticated roles:

- HSM Security Officer (SO)
  - Module-level role
  - Initializes and configures the module for operation
  - Creates user partitions
  - Configures the partition policy settings and performs security administration tasks within the user partition
  - Performs key management tasks for the admin partition
  - Performs cryptographic operations for the admin partition
  - Manages Crypto Officer and Crypto User roles

- Audit Officer (AO)
  - Module-level role
  - Initializes, configures, and manages secure audit logging

- Crypto Officer (CO)
  - User partition-level role
  - Performs key management tasks for the user partition
  - Performs cryptographic operations for the user partition

- Crypto User (User)
  - Optional user partition-level role
  - Performs cryptographic operations for the user partition

The module also supports the following unauthenticated role:

- Public User
  - Module-level and partition-level role which is permitted to access status information and perform diagnostics before authentication

The mapping of the cryptographic module's roles to the roles defined in FIPS 140-2 can be found in Table 2-2.

FIPS 140-2 Role	Luna T7 Cryptographic Module Role	Role Scope
Crypto Officer	HSM Security Officer (SO)	Module / Admin Partition / User Partition
	Audit Officer (AO)	Module
User	Crypto Officer (CO)	User Partition
	Crypto User	User Partition
Unauthenticated User	Public User	Module / Partition

TABLE 2-2: MAPPING OF FIPS 140-2 ROLES TO MODULE ROLES

2.3.2 Services

All services listed in Table 2-3 can be accessed in FIPS 140-2 Approved mode and non-Approved mode. The services listed in Table 2-3 use the security functions listed in Table 2-6, Table 2-7, Table 2-8, Table 2-9, and Table 2-10. When the module is operating in FIPS 140-2 Approved mode as described in Section 3.2, the non-Approved Security Functions in Table 2-10 are disabled and cannot

be used for these services. The non-Approved functions in Table 2-10 can only be accessed through the services when the module is in non-Approved mode.

Table 2-3: Roles and Access Rights by Service

Service	Cryptographic Keys and CSPs	Type of Access	Role				
			SO	CO	Crypto User	AO	Public User
Show Status	N/A	N/A	X	X	X	X	X
Self-test	N/A	N/A	X	X	X	X	X
Initialize Module	DRBG State	Use	X				
	Authentication data, SMK, PSK, KCV	Write					
Configure Module Policy	N/A	N/A	X				
Create Partition	N/A	N/A	X				
Initialize Partition	DRBG State	Use	X				
	Authentication data, USK, PSK, KCV	Write					
Configure Partition Policy	N/A	N/A	X				
Initialize Role	Authentication Data, USK, PSK	Write	X				
Login	Authentication Data, USK, PSK	Use					X
Logout	N/A	N/A	X	X	X	X	
Reset Role Authentication Data	Authentication Data, USK, PSK	Write	X				
Change Role Authentication Data	Authentication Data, USK, PSK	Use, Write	X	X	X	X	
Zeroize Module	Authentication data, SMK, PSK, KCV, LKCV, SADK, symmetric keys, asymmetric key pairs	Erase	X	X	X	X	X
Delete Partition	Authentication data, SMK, PSK, KCV, LKCV, SADK, symmetric keys, asymmetric key pairs	Erase	X				
Firmware Update	GSK, Root Certificate	Use, Write (firmware)	X				
Configuration Update	Root Certificate	Use	X				
	Authentication data, SMK, PSK, KCV, LKCV, SADK, symmetric keys, asymmetric key pairs	Erase (may invoke Zeroize)					
Generate Random Data	DRBG State	Use	X	X	X	X	
Key Generation	DRBG State	Use	X	X			
	Symmetric keys	Write					
Key Pair Generation	DRBG State	Use	X	X			
	Asymmetric key pairs	Write					
Domain Parameter Generation	DRBG State	Use	X	X			
	Domain Parameters	Write					

Table 2-3: Roles and Access Rights by Service							
Service	**Cryptographic Keys and CSPs**	**Type of Access**	**Role**				
			SO	**CO**	**Crypto User**	**AO**	**Public User**
Wrap/Unwrap Symmetric Key	Symmetric key, KTS asymmetric or symmetric wrapping key	Use, Write (unwrapped symmetric key)	X	X			
Wrap/Unwrap Asymmetric Key	Asymmetric key, KTS asymmetric or symmetric wrapping key	Use, Write (unwrapped asymmetric key)	X	X			
Key Agreement	Symmetric key, asymmetric key	Use, Write	X	X	X	X	
Key Derivation	Symmetric key	Use, Write	X	X	X	X	
Hash	N/A	N/A	X	X	X		
Partition Backup / Restore (Clone)	Asymmetric private keys, symmetric keys	Transfer/Clone	X	X			
	DRBG State, ROOT, MIC, HOC, TWC, TUK, KCV	Use					
Remote PED	DRBG State, RPV, Ephemeral ECDH private key, Symmetric key, HMAC key	Use	X	X	X	X	
	Ephemeral ECDH public key	Use, Write	X	X	X	X	
Symmetric Encrypt/Decrypt	DRBG State, Symmetric keys	Use	X	X	X		
Asymmetric Signature	DRBG State, RSA, DSA, ECDSA private keys	Use	X	X	X		
Asymmetric Verification	RSA, DSA, ECDSA public keys	Use	X	X	X		
Store Data Object	Non-cryptographic data	Write	X	X	X		X
Read Data Object	Non-cryptographic data	Read	X	X	X		X
Initialize Secure Audit Logging	DRBG State	Use				X	
	Authentication data, SADK	Write					
Change Audit Officer's Password	DRBG State	Use				X	
	Authentication data	Read, Write					
Configure Secure Audit Logging	N/A	Read, Write				X	
Synchronize Module Clock with Host System Clock	N/A	Write				X	
Verify, Import, and Export Secure Audit Log files	SALK	Use				X	
Show Secure Audit Log status	N/A	Read				X	
Import and Export the Wrapped Secure Audit Logging Key	SALK	Read, Write				X	

TABLE 2-3: ROLES AND ACCESS RIGHTS BY SERVICE

2.4 Authentication

All roles except for the Public User must authenticate to the module by providing their authentication data. Table 2-4 and Table 2-5 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 under this configuration, a module generates the authentication data as a 48-byte random value and writes it to a PED Key. Two-Factor Authentication, with PED Key plus a Challenge Secret password, is mandatory for the Crypto User role. The additional Challenge Secret password authentication can optionally be assigned to the Crypto Officer 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. In FIPS 140-2 Approved mode, the password is delivered to the module encrypted with the module's Password Encryption Key (PEC) using RSA-OAEP and a random nonce to prevent replay attacks.

Role	Type of Authentication	Authentication Data	
		Password Configuration	PED Configuration
HSM Security Officer	Identity-based	Password	Authentication Token (PED Key)
Crypto Officer	Identity-based	Password	Authentication Token (PED Key), plus optional Challenge Secret password
Crypto User	Identity-based	Password	Authentication Token (PED Key), plus mandatory Challenge Secret password
Audit Officer	Identity-based	Password	Authentication Token (PED Key)
Public User	Not Required	N/A	N/A

TABLE 2-4: ROLES AND REQUIRED IDENTIFICATION AND AUTHENTICATION

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}. With a maximum of 3 failed consecutive login attempts per minute for the SO and 10 for other Users, the threshold 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}. With a maximum of 3 failed consecutive login attempts per minute for the SO and 10 for other Users, the thresholds required by FIPS 140-2 can never be reached.

TABLE 2-5: STRENGTHS OF AUTHENTICATION MECHANISMS

2.4.1 Activation

If PED 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.

2.4.2 M of N

If PED is configured, the cryptographic module supports the use of an M of N secret sharing authentication scheme for each of the module roles. M of N authentication provides the capability to enforce multi-person integrity over the functions associated with each role.

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

2.5 Physical Security

The Luna T7 Cryptographic Module is a multi-chip embedded 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 Security Officer 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 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 Master Tamper Key (MTK) and the Token Variable Key (TVK), log the event, and halt operation. The module can be reset and placed back into operation when the external event signal is removed.

2.5.2 PCIe Card Removal

The module detects removal from the PCIe slot in both the powered-on state and the powered-off state. It is treated as an external event as described above. The Master Tamper Key (MTK) and Token Variable Key (TVK) are erased and the event is logged.

2.5.3 Decommission

The module supports a physical interface for the input of a decommission signal. The decommission signal 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), clear all working memory, log the event, and halt execution.

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 and placed back into operation when the decommission signal is removed, however it must be re-initialized.

2.5.4 Secure Transport Mode

The Luna T7 Cryptographic Module supports a command that will place the device in Secure Transport Mode that will disable processing with user key data while the device is in transit. This command erases the Master Tamper Key (MTK) stored in nonvolatile memory and sets status indicating the device is in Secure Transport Mode. Once the module reaches its destination, a secure recovery command can be issued, which will reconstitute the MTK. If configured, the Secure Recovery (Purple) PED Key is needed to provide part of the data to reconstruct the MTK.

2.5.5 EMI / EMC

The module is FCC Part 15 Class B Compliant for Conducted and Radiated Emissions.

2.5.6 Fault Tolerance

If power is lost for whatever reason, the module will 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.

The module will maintain its secure state 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.

2.5.7 Mitigation of Other Attacks

Timing attacks against the module are mitigated through the use of a hardware accelerator for modular exponentiation operations. The use of these hardware acceleration functions ensures that all RSA signature operations complete in very nearly the same time, therefore making the analysis of timing differences irrelevant. RSA blinding may also be selected as an option to mitigate this type of attack.

As described in Sections 2.5.1 and 2.5.3, the Luna T7 Cryptographic Module contains connectors for external signals to indicate tamper or decommission events. Section 2.5.2 also describes how the removal of the card from its PCI-Express slot, whether powered or not, is treated as a tamper event. In all of these cases, corresponding Critical Security Parameters (CSPs) are erased from nonvolatile memory based upon external signals provided by the appliance housing the module, such as the opening of the appliance housing.

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 in the Luna T7 Cryptographic Module can be found in the following tables. Some algorithms are implemented solely in firmware, some are implemented in hardware, and some are implemented in a combination of firmware and hardware.

Table 2-6: FIPS-Approved Algorithms, Luna T7 Hybrid (HW/FW) Cryptographic Library	
Approved Security Functions	**Certificate Number**
Symmetric Encryption/Decryption	
AES: CFB8 (Encrypt/Decrypt, Key Length: 128, 192, 256 bits)	C2010
Asymmetric	
RSA: Key Generation (186-4: 2048 and 3072-bit Modulo), Signature Generation[1] (186-4: 2048 and 3072-bit Modulo, SHA-1/SHA2-224/SHA2-256/SHA2-384/SHA2-512), Signature Verification (186-4: 1024, 2048, and 3072-bit Modulo, SHA-1/SHA2-224/SHA2-256/SHA2-384/SHA2-512) Signature Verification (186-2: 1024 and 1536-bit Modulo, SHA-1/SHA2-224/SHA2-256/SHA2-384/SHA2-512)	C2010
RSA (CVL): Decryption Primitive (2048-bit Modulus)	C2010
Key Agreement Scheme	
KAS (SP800-56B): KAS2-basic, RSASVE Generate, Recover per NIST SP800-56B	Vendor Affirmed
KAS-SSC (SP800-56Ar3): (Cofactor) Ephemeral Unified Model, C(2e, 0s, ECC CDH) Scheme, P-384 (secp384r1) Domain Parameters	Vendor Affirmed
Key Transport	
KTS (SP800-56B): KTS-OAEP-Basic, RSA-OAEP Encrypt, Decrypt per SP800-56B, SHA-512 Mask Generation Function	Vendor Affirmed
Key Derivation Function	
KBKDF (SP800-108): Counter Mode, CMAC-AES128/192/256	C2010
PBKDF (SP800-132): PKCS#5 PBKDF2, HMAC-SHA-1 per SP800-132 Option 1a	Vendor Affirmed
KDA (SP800-56Cr1): Extraction-then-Expansion KDF**.** The two-step key derivation is performed per Section 5.1 of SP800-56Cr1 with AES-128-CMAC as the Auxiliary MAC algorithm for Randomness Extraction and AES-128-CMAC as the Auxiliary PRF-based KDF for Key Expansion.	Vendor Affirmed

TABLE 2-6: FIPS-APPROVED ALGORITHMS, LUNA T7 HYBRID (HW/FW) CRYPTOGRAPHIC LIBRARY

[1] FIPS 186-4 SigGen testing at 4096-bit modulus was not made available until ACVP was later developed and 4096-bit testing was only available in FIPS 186-2 form via CAVS. Hence, this module has been tested for FIPS 186-4 SigGen for modulus less than 4096 (2048 and 3072), but only tested SigGen with FIPS 186-2 at 4096 bits; this was done as an added assurance rather than claiming compliance to FIPS 186-2.

Table 2-7: FIPS-Approved Algorithm Implementations, Luna T7 Hardware Cryptographic Engine	
Approved Security Functions	**Certificate Number**
Symmetric Encryption/Decryption	
AES: ECB, CBC, OFB, CTR, CFB128, GCM[2] (also GMAC), KW, KWP (All modes above: Encrypt/Decrypt, Key Length: 128, 192, 256 bits) XTS[3] (Encrypt/Decrypt, Key Length: 128, 256 bits)	C1999
Hashing	
SHS (Secure Hash Standard): SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	C1999
Message Authentication Code	
HMAC: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	C1999
AES: CMAC (Generation/Verification, Key Length: 128, 192, 256 bits)	C1999
Asymmetric	
DSA: Parameter Generation (PQGGen, 186-4: 2048/224, 2048/256, 3072/256), Key Generation (186-4: 2048/224, 2048/256, 3072/256), Signature Generation (186-4: 2048/224, 2048/256, 3072/256), Signature Verification (186-4: 1024/160, 2048/224, 2048/256, 3072/256)	C1999
ECDSA: Key Generation (186-4), Signature Generation (186-4), Signature Verification (186-4) Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 Hash Algorithms (all Curves): SHA2-224, SHA2-256, SHA2-384, SHA2-512)	C1999

[2] The module's AES-GCM implementation conforms to IG A.5 Technique #2.

The IV is generated internally by the module using Approved Hash_DRBG (SHA-256) being generated inside the module's physical boundary.

The IV generation supported in FIPS Approved mode is fixed 96-bit size that is generated with the SP800-90A Hash_DRBG (SHA-256) output.

Since the IV is generated internally and is random and is fixed 96 bits in length, requirements from IG 7.15 are satisfied.

[3] The check for Key_1 ≠ Key_2 is done before using the keys in the XTS-AES algorithm to process data and is in accordance with IG A.9 requirements.

Table 2-7: FIPS-Approved Algorithm Implementations, Luna T7 Hardware Cryptographic Engine	
Approved Security Functions	**Certificate Number**
Key Transport	
KTS (AES Cert. #C1999): An implementation has been tested for its compliance with AES KW and/or AES KWP and this mode of AES is used for key wrapping.	C1999
Key Generation	
CKG (Cryptographic Key Generation)[4]	Vendor Affirmed
Random Number Generation – RNG4 4.2	
SHS (Secure Hash Standard) SHA-256, Message Length: 8-51200, Increment 8	SHS 2112
DRBG Hash_DRBG, SHA-256 with Prediction Resistance Support Prerequisites: SHS 2112	DRBG 349

TABLE 2-7: FIPS-APPROVED ALGORITHM IMPLEMENTATIONS, LUNA T7 HARDWARE CRYPTOGRAPHIC ENGINE

Table 2-8: FIPS-Approved Algorithm Implementations, Luna T7 Firmware Cryptographic Library	
Approved Security Functions	**Certificate Number**
Symmetric Encryption/Decryption	
AES: ECB, CBC, OFB (All modes: Encrypt/Decrypt, Key Length: 128, 192, 256 bits)	C1998
TDES (Decrypt): CBC	C1998
Hashing	
SHS (Secure Hash Standard): SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	C1998

TABLE 2-8: FIPS-APPROVED ALGORITHM IMPLEMENTATIONS, LUNA T7 FIRMWARE CRYPTOGRAPHIC LIBRARY

[4] Resulting symmetric keys and seeds used for asymmetric key generation are an unmodified output from Approved Hash_DRBG.

Table 2-9: Non-Approved, But Allowed Security Functions	
Allowed Security Functions	**Description**
Random Number Generation	
NDRNG, Entropy Source #1 [5]	This entropy source is available on both Luna T7 hardware module variants (872-500024-001 and 872-500025-001). It is the only entropy source available on the 872-500024-001; it can be configured as the entropy source on the 872-500025-001 by a module policy setting under the control of the SO. There is no scenario where both entropy sources are utilized at the same time. It is used for seeding the Hash_DRBG per IG 7.14 scenario 1 (a). This noise source provides 256 bits of entropy for the Hash_DRBG Instantiation and meets the requirements of IG 7.15. [6]
NDRNG, Entropy Source #2 [5] **(Quantum Entropy Source)**	This entropy source is available only on the T7 872-500025-001 hardware module. It can be configured as the entropy source by a module policy setting under the control of the SO. There is no scenario where both entropy sources are utilized at the same time. It is used for seeding the Hash_DRBG per IG 7.14 scenario 1 (a). The noise source provides 256 bits of entropy for the Hash_DRBG Instantiation and meets the requirements of IG 7.15. [6]

TABLE 2-9: NON-APPROVED, BUT ALLOWED SECURITY FUNCTIONS

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 3.2.

Table 2-10: Non-FIPS Approved Security Functions
Symmetric Encryption/Decryption
DES
Triple-DES (Encrypt)
RC2
RC4
RC5
CAST5
Hashing
MD2
MD5
Message Authentication Code
AES MAC (non-compliant)
DES-MAC
RC2-MAC
RC5-MAC
RIPEMD-160
CAST3-MAC
CAST5-MAC
SSL3-MD5-MAC
SSL3-SHA1-MAC
HMAC (non-compliant less than 112 bits of encryption strength)

[5] There is only one Entropy Source active at any time on any Luna T7 Cryptographic Module. On the T7 872-5000025-001 Hardware Module, where either Entropy Source can be configured as active by module policy, when one source is selected to provide entropy to the DRBG, the other is inactive. **There is no mixing of these two Entropy Sources as input data.**

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

Table 2-10: Non-FIPS Approved Security Functions
Asymmetric
RSA X-509
RSA (non compliant less than 112 bits of encryption strength)
DSA (non-compliant less than 112 bits of encryption strength)
ECDSA (non-compliant less than 112 bits of encryption strength)
Generate Key
DES
Triple-DES
RC2
RC4
RC5
CAST3
CAST5
SSL PRE-MASTER
Key Agreement
ECC (non-compliant less than 112 bits of encryption strength)
Diffie-Hellman (key agreement; key establishment methodology; non-compliant less than 112 bits)
Key Transport
RSA (key wrapping; key establishment methodology; non-compliant less than 112 bits of encryption strength)

TABLE 2-10: NON-FIPS APPROVED SECURITY FUNCTIONS

2.7.3 Cryptographic Keys and Critical Security Parameters

Keys and CSPs	CSP Type	Generation	Input / Output	Description
Challenge Secret	16 character data string	SHA-256 Hash_DRBG	Output via direct connection to PED	Used in Trusted Path Authentication configuration. 16 character random string generated by the cryptographic module and output via the PED display when the user is created. It is input by the operator as the authentication data for a client application login.
Random Challenge	64-byte random number	SHA-256 Hash_DRBG	Output to host using ICD communication path	Used in Trusted Path Authentication configuration. A one-time random number generated by the cryptographic module and sent to the calling application for each login. It is combined with the input Challenge Secret to compute the one-time response that is returned to the cryptographic module.
Challenge Response	20-byte value	N/A	Input from host using ICD communication path	A 20-byte value used for authentication in the challenge response scheme. It is generated using the challenge secret and the one-time random challenge value.
PED Key Authentication Data	48-byte random value	SHA-256 Hash_DRBG	Input / Output via direct connection to PED	Used in Trusted Path Authentication configuration. A 48-byte random value that is generated by the module when the SO or User is created. It is written out to the serial memory device (PED Key) via the Trusted Path.
Optional PIN	4-48 character PIN	N/A	Input on the PED via secure channel. PED does not input or output the PIN.	An optional PIN value used for authentication along with the PED key. It must be a minimum of 4-bytes long
Cloning Domain Vector / Key Cloning Vector (KCV)	48-Byte value	SHA-256 Hash_DRBG	Output via direct connection to PED	48-byte value that is used to control a module's ability to participate in the cloning protocol. It is either generated by the module or imprinted onto the module at the time the module is initialized. The value is output from the original module in the domain onto a PED Key to enable initializing additional modules into the same domain.
User Storage Key (USK)	AES-256 ECB	SHA-256 Hash_DRBG	Not Input or Output	This key is used to encrypt all sensitive attributes of all private objects owned by the User. Encrypted, as part of the UAV, by the key taken from the PED Key data.
Security Officer Master Key (SMK)	AES-256 ECB	SHA-256 Hash_DRBG	Not Input or Output	The storage key for the SO. This key is used to encrypt all sensitive attributes of all private objects owned by the SO. The USK/SMK is stored encrypted by an AES key derived from the User/SO PED Key Authentication data.
Global Storage Key (GSK)	AES-256 ECB	SHA-256 Hash_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.
Secondary Global Storage Key (SGSK)	AES-256 ECB	SHA-256 Hash_DRBG	Not Input or Output	It is used to encrypt non-permanent parameters – parameters re-generated for every module initialization.
Token or Module Unwrapping Key (TUK)	RSA-4096 bit private key	FIPS 186-4 RSA Key Generation, input from SHA-256 Hash_DRBG	Not Input or Output	Current version (v4) of the 4096-bit RSA private key used in the cloning protocol for FIPS mode. It is generated on power-up if it does not exist.
Token or Module Wrapping Certificate (TWC)	RSA-4096 public key certificate	FIPS 186-4 RSA Key Generation, input from SHA-256 Hash_DRBG	Output in plaintext using ICD communication path	Current version (v4) of the public key certificate used in the KAS2-basic Key Agreement Scheme for the session encryption key as part of the cloning protocol in FIPS mode. It is generated on power-up and signed by the HOK.
Password Encryption Key (PEK)	RSA-4096 bit private key	FIPS 186-4 RSA Key Generation, input from SHA-256 Hash_DRBG	Not Input or Output	A 4096 bit RSA private key used to decrypt user passwords that are provided to the module. It is generated on power-up if it does not exist.

Keys and CSPs	CSP Type	Generation	Input / Output	Description
Password Encryption Certificate (PEC)	RSA-4096 public key certificate	FIPS 186-4 RSA Key Generation, input from SHA-256 Hash_DRBG	Output in plaintext using ICD communication path	The X.509 public key certificate corresponding to the PEK. The PEC is provided to the host as part of the KTS-OAEP-Basic scheme for secure transport of password data. It is generated on power-up and signed by the HOK.
U2 Key	32-byte generic secret key	SHA-256 Hash_DRBG	Not Input or Output	32-byte symmetric key used in conjunction with the authentication code for a firmware update to derive a key used to decrypt the firmware update image when it is loaded into the module.
Token or Module Variable Key (TVK)	AES-256 ECB	SHA-256 Hash_DRBG	Not Input or Output	It is used to encrypt cached User authentication data when auto-activation is enabled. The non-volatile RAM storing the TVK is actively zeroized in response to a tamper event.
Master Tamper Key (MTK)	AES-256 ECB	SHA-256 Hash_DRBG	Not Input or Output	The MTK encrypts all sensitive values for use in the cryptographic accelerators. The non-volatile RAM storing the MTK is actively zeroized in response to a tamper event.
Key Encryption Key (KEK)	AES-256 ECB	SHA-256 Hash_DRBG	Not Input or Output	The KEK encrypts all sensitive values and is zeroized in response to a decommission signal.
Root Certificate (ROOT)	RSA-4096 public key certificate	Loaded at manufacturing	Input (at manufacture) and output in plaintext using ICD communication path	The X.509 public key certificate corresponding to the Thales TCT Root signing key. It is self-signed. Used in verifying Manufacturing Integrity, Firmware, and License Signing Certificates (MIC, FSC, and LSC).
Manufacturer's Integrity Certificate (MIC)	RSA-4096 public key certificate	Loaded at manufacturing	Input (at manufacture) and output in plaintext using ICD communication path	Used in verifying Hardware Origin Certificates (HOCs), which are generated in response to a customer function call to provide proof of hardware origin. It is signed by the Root Key.
Firmware Signing Certificate (FSC)	RSA-4096 public key certificate	Delivered with Firmware Update Package	Input in plaintext using ICD communication path	The X.509 public key certificate corresponding to the Firmware Signing Key (FSK). It is input in plaintext as part of the Firmware Update File (FUF). It is signed by the Thales TCT Root signing key. Used to verify Firmware images on initial load.
License Signing Certificate (LSC)	RSA-4096 public key certificate	Delivered with Configuration Update Package	Input in plaintext using ICD communication path	The X.509 public key certificate corresponding to the License Signing Key (LSK). It is input in plaintext as part of the Configuration Update File (CUF). It is signed by the Thales TCT Root signing key. Used to verify Configuration Update images on initial load.
Device Authentication Key (DAK)	RSA-4096 bit private key	FIPS 186-4 RSA Key Generation, input from SHA-256 Hash_DRBG	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 Certificate (DAC)	RSA-4096 public key certificate	FIPS 186-4 RSA Key Generation, input from SHA-256 Hash_DRBG	Output in plaintext using ICD communication path	The X.509 public key certificate corresponding to the DAK. It is 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.
Manufacturing Authentication Certificate (MAC)	RSA-4096 public key certificate	Loaded at manufacturing	Input (at manufacture) and output in plaintext using ICD communication path	Used in verifying Device Authentication Certificate (DAC). MAC is loaded at manufacturing to provide Manufacturing authentication.
Hardware Origin Key (HOK)	RSA-4096 bit private key	FIPS 186-4 (ANSI X9.31) RSA Key Generation, input from SHA-256 Hash_DRBG	Not Input or Output	RSA private key used to sign certificates for other device messaging key pairs, such as the TWC. It is generated at the time the device is manufactured.

Keys and CSPs	CSP Type	Generation	Input / Output	Description
Hardware Origin Certificate (HOC)	RSA-4096 public key certificate	Loaded at manufacturing	Input (at manufacture) and output in plaintext using ICD communication path	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.
Remote PED Vector (RPV)	256-bit secret value	SHA-256 Hash_DRBG	Output via direct connection to 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.
Secure Recovery Vector (SRV)	Split of AES-256 MTK	SHA-256 Hash_DRBG	Input / Output via direct connection to PED	A split of the MTK that is written to one or more PED Keys using the M of N secret splitting scheme and used to recover the MTK after a tamper event has been cleared.
DRBG C	440 bits	SHA-256 Hash_DRBG	Not Input or Output	Hash_DRBG Constant state variable, dependent upon the Seed, that is stored ephemerally in unreadable RNG register space and updated on each Instantiate and Reseed operation in accordance with NIST SP 800-90A.
DRBG V	440 bits	SHA-256 Hash_DRBG	Not Input or Output	Hash_DRBG Value state variable that is stored ephemerally in unreadable RNG register space and updated on each Instantiate, Generate, and Reseed operation in accordance with NIST SP 800-90A.
DRBG Entropy Input	256 bits	Hardware Random Source	Not Input or Output	The entropy value used to Instantiate and Reseed the approved Hash_DRBG. This value is stored ephemerally in unreadable RNG register space. 256 bits are used for Seed and 128 bits are used for Nonce as needed. An additional 256 bits of random Personalization Data are added on an Instantiate and 256 bits of random Additional Information are added on a Reseed.
Secure Audit Logging Key (SALK)	256-bit HMAC	SHA-256 Hash_DRBG	Input and output encrypted using ICD communication path	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 Domain Key (SADK)	AES-256 KW	SHA-256 Hash_DRBG	Input / Output via direct connection to PED	A 256-bit key that is used to wrap/unwrap the SALK when it is exported from / imported 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.

TABLE 2-11: KEYS AND CRITICAL SECURITY PARAMETERS USED IN THE MODULE

2.7.4 Key Generation

In accordance with FIPS 140-2 Implementation Guidance (IG) D.12, the cryptographic module performs Cryptographic Key Generation (CKG) in compliance with scenario 1 of Section 4 in SP800-133r2. Symmetric cryptographic keys are generated by the direct unmodified output of the module's NIST SP800-90A DRBG. The DRBG output is also used as a seed for asymmetric key generation.

Keys which are generated outside the module and input during the manufacturing process include:
Root Certificate (ROOT), Manufacturer's Integrity Certificate (MIC), Hardware Origin Certificate (HOC), Manufacturing Authentication Certificate (MAC).

User passwords for authentication are generated by the operator.

2.7.5 Key Import and Export

If PED is configured, the following keys/CSPs use the module's direct connection to the PED for entry/output: PED Authentication Data, Cloning Domain Vector (KCV), Remote PED Vector (RPV), Secure Recover Vector (SRV), and Secure Audit Domain Key (SADK).

In both configurations, the following keys/CSPs use the ICD communication path to the host for entry/output: All certificates, Authentication Nonce, User Password and Secure Audit Logging Key (SALK).

The remaining keys and CSPs listed in Table 2-11 are not input to or output from the module.

Depending on the configuration of the module, the following methods of key import and export may be available as a service:

2.7.5.1 Key Cloning

Key cloning uses a one-time AES key as a session key to wrap (AES-KWP) an object being transferred from one cryptographic module to another. Objects transferred using the cloning protocol may be keys, user data, or module data. The AES session encrypting key is obtained by using KAS2-basic as the key agreement scheme between source and target modules, both of which share their Token Wrapping Certificates (TWCs). Both parties use the agreed upon shared secret in a Two-Step Key Derivation Function with Randomness Extraction per SP800-56Cr1 and SP800-108, with the distributed Key Cloning Vector (KCV) as part of the FixedInput, to derive matching session keys for the wrapping and unwrapping operations.

2.7.5.2 Key Wrap / Unwrap

The key wrap operation encrypts an asymmetric or symmetric key value for output, using AES-KW symmetric wrapping key.

The unwrap operation takes as input an encrypted symmetric or asymmetric private key and a handle to the key that was originally used to do the wrapping. It decrypts the key, stores it in the module as a key object and returns the handle to the imported key.

Note that for both wrap and unwrap operations, the user (or calling application acting on the user's behalf) never has access to the actual key values – only handles assigned to the key objects in the module.

2.7.6 Zeroization

The module supports the following zeroization methods for plaintext keys and CSPs.

Zeroization Method	Events	Description
ZM1	- Zeroized by power cycle or module reset	Power-on reset initialization and test of RAM space
ZM2	- Zeroized in response to physical security measures (Tamper)	Erasure of MTK in Nonvolatile RAM
ZM3	- Zeroized as part of a Decommission signal	Erasure of KEK, TVK, and MTK in Nonvolatile RAM
ZM4	- Zeroized via ICD command - Zeroized when moving to/from FIPS 140-2 Approved mode and non-Approved mode of operation - Zeroized when the configured threshold for failed SO login attempts is reached	Execution of firmware zeroize function that deletes all user cryptographic objects stored in nonvolatile module memory and deletes all user keys (USK, SMK) and partitions. Module is in its factory reset state and must be re-initialized.

TABLE 2-12: ZEROIZATION METHODS

2.8 Self-tests

2.8.1 Power-On Self-Tests

The module provides self-tests on power-up and on request to confirm the firmware integrity, and to check the random number generator and each of the implemented cryptographic algorithms. All interfaces and external operations are disabled until the Power-On Self-Tests complete successfully.

Table 2-13: Power-On Self-Tests, Module Integrity			
Test	**When Performed**	**Where Performed**	**Indicator**
Bootloader performs a SHA-1 integrity check of bootloader image	Power-on	Firmware	Module halt
Bootloader performs a SHA-256 integrity check of firmware image	Power-on	Firmware	Module halt

TABLE 2-13: POWER-ON SELF-TESTS, MODULE INTEGRITY

Table 2-14: Power-On Self-Tests, Cryptographic Implementations					
Test	**When Performed**	**Where Performed**			**Indicator**
		Luna T7 Hybrid (HW/FW) Cryptographic Library (CAVP Cert. #C2010)	**Luna T7 Hardware Cryptographic Engine (CAVP Cert. #C1999)**	**Luna T7 Firmware Cryptographic Library (CAVP Cert. #C1998)**	
DRBG Instantiate Function Known Answer Test (KAT)	Power-on/Request		X		Module halt / Error Logged
DRBG Generate Function KAT	Power-on/Request		X		Module halt / Error Logged
DRBG Reseed Function KAT	Power-on/Request		X		Module halt / Error Logged
DRBG Uninstantiate Function KAT	Power-on/Request		X		Module halt / Error Logged
SHA-1 KAT	Power-on/Request		X	X	Module halt / Error Logged
SHA-224 KAT	Power-on/Request		X	X	Module halt / Error Logged
SHA-256 KAT	Power-on/Request		X	X	Module halt / Error Logged
SHA-384 KAT	Power-on/Request		X	X	Module halt / Error Logged
SHA-512 KAT	Power-on/Request		X	X	Module halt / Error Logged
HMAC SHA-1 KAT	Power-on/Request		X		Module halt / Error Logged
HMAC SHA-224 KAT	Power-on/Request		X		Module halt / Error Logged
HMAC SHA-256 KAT	Power-on/Request		X		Module halt / Error Logged
HMAC SHA-384 KAT	Power-on/Request		X		Module halt / Error Logged
HMAC SHA-512 KAT	Power-on/Request		X		Module halt / Error Logged
RSA sig-gen KAT	Power-on/Request	X			Module halt / Error Logged
RSA sig-ver KAT	Power-on/Request	X			Module halt / Error Logged
RSA Encrypt KAT	Power-on/Request	X			Module halt / Error Logged
RSA Decrypt KAT	Power-on/Request	X			Module halt / Error Logged
DSA sig-gen KAT	Power-on/Request		X		Module halt / Error Logged
DSA sig-ver KAT	Power-on/Request		X		Module halt / Error Logged
AES KATs (e / d) (ECB, CBC, OFB)	Power-on/Request		X	X	Module halt / Error Logged

Table 2-14: Power-On Self-Tests, Cryptographic Implementations					
Test	When Performed	Where Performed			Indicator
		Luna T7 Hybrid (HW/FW) Cryptographic Library (CAVP Cert. #C2010)	Luna T7 Hardware Cryptographic Engine (CAVP Cert. #C1999)	Luna T7 Firmware Cryptographic Library (CAVP Cert. #C1998)	
AES KATs (e / d) (CTR, CFB128, GCM, XTS)	Power-on/Request		X		Module halt / Error Logged
AES-CFB8 KAT (e / d)	Power-on/Request	X			Module halt / Error Logged
AES-CMAC KAT	Power-on/Request		X		Module halt / Error Logged
TDES-CBC KAT (Decrypt)	Power-on/Request			X	Module halt / Error Logged
ECDSA sig-gen KAT	Power-on/Request		X		Module halt / Error Logged
ECDSA sig-ver KAT	Power-on/Request		X		Module halt / Error Logged
KBKDF KAT	Power-on/Request	X			Module halt / Error Logged

TABLE 2-14: POWER-ON SELF-TESTS, CRYPTOGRAPHIC IMPLEMENTATIONS

2.8.2 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 2-15: Conditional Self-Tests			
Test	When Performed	Where Performed	Indicator
CRNGT test for NDRNG[7]	Continuous	Firmware / Hardware	Function Fail / Error Logged
RSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware / Hardware	Function Fail
DSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware / Hardware	Function Fail
ECDSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware / Hardware	Function Fail
Firmware load test (4096-bit RSA sig ver)	On firmware update load	Firmware / Hardware	Function Fail / Error Logged Module will continue with existing firmware

TABLE 2-15: CONDITIONAL SELF-TESTS

2.9 Firmware Security

The Firmware Security Policy assumes that any firmware images loaded in conformance with the policy have been verified by Thales TCT to ensure that the firmware will function correctly. The policy applies to initial firmware loading and subsequent firmware updates.

The module does not allow external software to be loaded inside its boundary. Only properly formatted firmware may be loaded. The communication of initial or updated firmware to a target module shall be initiated by a Thales TCT module dedicated to that function.

[7] 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 SP800-90A.

Firmware shall be digitally signed using the Thales TCT Manufacturing signature key and encrypted using a secret key that can be derived (based on an internally held secret key) by the receiving module for decryption. RSA (4096 bits) PKCS #1 V1.5 with SHA-384 is used as the approved signature method. The unencrypted firmware must not be visible outside a module before, during and after the loading operation.

The Bootloader provides a SHA-1 integrity check (160-bit EDC) of itself and a SHA-256 integrity check (256-bit EDC) of the Firmware it loads on each power-on and reset cycle. The module will halt if either integrity check fails.

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. 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 validation.

3.1.1 Checking The Bootloader Version

The bootloader version can be checked by viewing the output from `dmesg` which can be run on the Linux based host platform following boot of the cryptographic module. The bootloader version will be listed towards the top of the data output on a line similar to below:

```
[hsm] Boot Loader Revision T7 2.0.1.
```

3.1.2 Checking The Hardware Model and Firmware Version

The Luna T7 hardware model and firmware version can be displayed by the `lunacm` utility running on the module host. The `lunacm slot list` command provides an output similar to the following, including the hardware model and firmware version:

```
lunacm:>slot list
Slot Id -> 3
Label -> Luna T7 Demo Partition
Serial Number -> 700021
Model -> Luna T7
Firmware Version -> 7.11.1
Configuration -> Luna PCI (PED) Key Export With Cloning Mode
```

Note: As indicated in Table 2-3, this module supports a Firmware Update service. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

3.2 Approved Mode Of Operation

The cryptographic module is approved when running a FIPS 140-2 certified version of firmware as listed in Section 1.

To place the module in FIPS 140-2 Approved mode as defined by FIPS PUB 140-2, the HSM Security Officer must disable the following module policy:

- “Execute in non-FIPS operation mode”

If the HSM Security Officer attempts to enable or disable this policy, a warning is displayed and the HSM Security Officer is prompted to confirm the selection. If this policy is left in the “enabled” state, the module will be operating in the non-Approved mode.

The HSM Security Officer can confirm that the cryptographic module is in FIPS 140-2 Approved mode by executing the `lunacm hsm showinfo` command in the administration tools provided with the module. If the module is in FIPS 140-2 Approved mode the following message will be displayed:

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

When not in FIPS 140-2 Approved mode, the showinfo status will not include that message.

3.2.1 Transitioning to and from FIPS Mode of Operation

If the “Execute in non-FIPS operation mode” policy is “enabled”, the Security Officer can use the `lunacm` tool to change that policy to “disabled” by use of the `hsm changepolicy` command to place the T7 module in the Approved FIPS Mode of Operation. As noted in Section 2.7.6, this will result in a Software Zeroization (ZM4) that will erase all users, partitions, and cryptographic objects.

To complete the process of Zeroization for enabling FIPS Mode, the user should also press the available button or switch to execute a Decommission (ZM3) to erase the contents of nonvolatile RAM and then cycle power to the device to perform a power-up initialization (ZM1) as well.

If the need should arise to exit the Approved FIPS Mode of Operation, the process above is repeated, except that the “Execute in non-FIPS operation mode” policy is set to “enabled” to perform the Software Zeroization (ZM4), which is then followed by the Decommission (ZM3) and Power-On Reset (ZM1) zeroizations.

APPENDIX A. LIST OF TERMS, ABBREVIATIONS AND ACRONYMS

Term	Definition
ANSI	American National Standards Institute
CL	Cloning (a capability configuration used to allow the secure transfer of key objects from one module to another for backup and restore and object replication purposes).
CLI	Command Line Interface
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem
CSP	Critical Security Parameter
CU	Crypto User
CUF	Configuration Update File
DAK	Device Authentication Key
DH	Diffie Hellman
DRNG	Deterministic Random Number Generator
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
EDC	Error Detection Code
FIPS	Federal Information Processing Standard
FUF	Firmware Update File
GSK	Global Storage Key
HA	High Assurance
HOC	Hardware Origin Certificate
HOK	Hardware Origin Key
HRNG	Hardware Random Number Generator
HSM	Hardware Security Module
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KEK	Key Encryption Key
MAC	Message Authentication Code
MIC	Manufacturer's Integrity Certificate
MIK	Manufacturer's Integrity Key
MTK	Master Tamper Key
PCI	Peripheral Component Interconnect
PED	PIN Entry Device
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
RNG	Random Number Generator
RPED	Remote PED
RPK	Remote PED Key
RPV	Remote PED Vector
SA	Server-Attached

Term	Definition
SADK	Secure Audit Domain Key
SALK	Secure Audit Logging Key
SGSK	Secondary Global Storage Key
SHS	Secure Hash Standard
SMK	Security Officer's Master Key
SO	Security Officer
SRK	Secure Recovery Key
TUK	Token or Module Unwrapping Key
TVK	Token or Module Variable Key
TWC	Token or Module Wrapping Certificate
USK	User's Storage Key