Thales Trusted Cyber Technologies

Luna T7

FIPS 140-3 Level3 Security Policy – Non-Proprietary

Trademarks, Copyrights, and Third-Party Software

© 2026 SafeNet Assured Technologies, LLC. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

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 copied or distributed 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.

Document Information

Document Part Number	002-500027-001
Release Date	May 1, 2026

Revision History

Revision	Date	Reason
A	September 11, 2024	Document baseline.
B	December 11, 2024	Update after first lab review.
C	January 6, 2025	Added authentication objective. Added meaning of characters G, R, W, E, Z used in the SSP Access column of the Approved Services table.
D	February 28, 2025	Removed Physical Trusted Path – Backup HSM section. It is not used in this version of the module. General review and update addressing reviewer comments
E	April 21, 2025	Updates from certification lab. Received on April 14th. Updates include removing CU from the Import Public Key service, changing “Audit User” to “Audit Officer”, Updating the ACVP algorithm certs.
F	January 14, 2026	Updates to include the supported PQC algorithms (ML-DSA and ML-KEM). Updates to include HMAC algorithms for Key-Based KDF security function. Corrected the Initialize Remote PED Vector service.
G	April 14, 2026	Updates to address CMVP comments. Removal of non-approved mode and trusted channel.

Table of Contents

Trademarks, Copyrights, and Third-Party Software 2
Disclaimer 2

1 General 8
1.1 Overview 8
1.2 Security Levels 9

2 Cryptographic Module Specification 10
2.1 Description 10
2.2 Tested and Vendor Affirmed Module Version and Identification 11
2.3 Excluded Components 11
2.4 Modes of Operation 11
2.5 Algorithms 12
2.5.1 Approved Algorithms 12
2.5.2 Vendor-Affirmed Algorithms 17
2.6 Security Function Implementations 18
2.7 Algorithm Specific Information 24
2.7.1 AES-GCM IV Generation 24
2.7.2 PBKDF 24
2.7.3 XTS-AES 24
2.8 RBG and Entropy 24
2.8.1 Thales Luna T7 Entropy Source 24
2.8.2 IDQ Quantis IID QRNG 25
2.8.3 Entropy buffer 25
2.8.4 DRBG Seeding and reseeding 25
2.8.5 RBG Output 25
2.9 Key Generation 25
2.10 Key Establishment 25
2.10.1 Key Import and Export 25
2.10.2 Key Cloning 26
2.10.3 Key Transport 26
2.10.4 Key Agreement 26
2.10.5 Key establishment mechanisms 26
2.11 Industry Protocols 26

3 Cryptographic Module Interfaces 27
3.1 Ports and Interfaces 27

4 Roles, Services, and Authentication 29
4.1 Authentication Methods 29
4.1.1 Identity 30
4.1.2 Activation 30
4.1.3 M of N 30
4.1.4 PED Keys 31
4.2 Roles 31
4.3 Approved Services 32
4.3.1 HSM Set Policy service 59
4.3.2 Partition Set Policy service 59
4.3.3 Configuration update service 59

4.3.4 Audit Config service 59
4.4 Non-Approved Services 59
4.5 External Firmware Loaded 59

5 Firmware Security 60
5.1 Integrity Techniques 60
5.2 Initiate on Demand 60

6 Operational Environment 61
6.1 Operational Environment Type and Requirements 61

7 Physical Security 62
7.1 Mechanisms and Actions Required 62
7.5 EFP/EFT Information 62
7.6 Hardness Testing Temperature Ranges 62
7.7 Additional Information 63
7.7.1 Secure Transport Mode 63
7.7.2 Temperature ranges 63

8 Non-Invasive Security 64

9 Sensitive Security Parameters Management 65
9.1 Storage Areas 65
9.2 SSP Input-Output Methods 65
9.3 SSP Zeroization Methods 65
9.4 SSPs 67
9.5 Transitions 76

10 Self-Tests 77
10.1 Pre-Operational Self-Tests 77
10.2 Conditional Self-Tests 78
10.3 Periodic Self-Test Information 83
10.4 Error States 85
10.5 Operator Initiation of Self-Tests 85

11 Life-Cycle Assurance 86
11.1 Installation, Initialization, and Startup Procedures 86
11.1.1 Installation 86
11.1.2 Initialization 86
11.2 Administrator Guidance 87
11.2.1 PED Key management 87
11.3 Non-Administrator Guidance 87
11.6 End of Life 88

12 Mitigation of Other Attacks 89
12.1 Attack List 89

List of Tables

Table 1: Security Levels 9
Table 2: Tested Module Identification – Hardware 11
Table 3: Modes List and Description 11
Table 4: Approved Algorithms - Firmware 14
Table 5: Approved Algorithms - Hybrid 17
Table 6: Vendor-Affirmed Algorithms 17
Table 7: Security Function Implementations 23
Table 8: Entropy Certificates 24
Table 9: Entropy Sources 24
Table 10: Ports and Interfaces 27
Table 11: Authentication Methods 29
Table 12: Roles 31
Table 13: Approved Services 58
Table 14: Mechanisms and Actions Required 62
Table 15: EFP/EFT Information 62
Table 16: Hardness Testing Temperatures 62
Table 17: Storage Areas 65
Table 18: SSP Input-Output Methods 65
Table 19: SSP Zeroization Methods 66
Table 20: SSP Table 1 71
Table 21: SSP Table 2 75
Table 22: Pre-Operational Self-Tests 77
Table 23: Conditional Self-Tests 82
Table 24: Pre-Operational Periodic Information 83
Table 25: Conditional Periodic Information 84
Table 26: Error States 85

List of Figures

Figure 1 Luna PCIe HSM (T-Series) 8
Figure 2 Luna Network HSM (T-Series) with Luna PCIe HSM (T-Series) Installed 8
Figure 3 Luna T7 (872-500025-001) 11
Figure 4 Luna T7U (875-500025-002) 11
Figure 5 Luna T7 Physical Ports 27
Figure 6 Luna T7 PCI Bracket View 28
Figure 7 PIN Entry Device (PED) and PED Keys 30

1 General

1.1 Overview

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

This document applies to Luna T7 Cryptographic Module. Hereafter referred to as the Luna T7.

The Luna T7 is available as a stand-alone product, the Luna PCIe HSM (T-Series) (Figure 1), to install in a user's Windows or Linux host or embedded within other products. Examples of other products include:

- The Luna Network HSM (T-Series) (Figure 2)
- The CipherTrust Manager k570

Figure 1 Luna PCIe HSM (T-Series)

Figure 2 Luna Network HSM (T-Series) with Luna PCIe HSM (T-Series) Installed

The security policies described in this document apply to the Luna T7 only and not to any products using the module.

1.2 Security Levels

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	3
	Overall Level	3

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Luna T7 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 (i.e. Luna Network HSM T-Series appliance).

A Luna T7 provides secure key generation and storage for symmetric keys and asymmetric key pairs along with support for a broad range of 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 Luna T7 must be configured to operate in the approved mode per section 11.1.2. Failure to configure the Luna T7 in this manner means the module will be providing services using non-approved cryptography, and is not confirming to the capabilities described in this document.

A Luna T7 may host multiple user partitions to store symmetric keys and asymmetric key-pairs. User partitions are cryptographically isolated from one another. Authentication is unique to a user partition and the contents of a partition is only available to the authenticated user.

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

For configuring the mode of operation of the Luna T7 installed within a user's Windows or Linux host, a software application, lunacm, is provided. lunacm uses the module's proprietary command interface (ICD) to configure the module's mode of operation. To configure the mode of operation of a Luna T7 installed within a Luna Network HSM T-Series, Luna Shell (lunash) is provided. Using SSH, lunash is available to the administrator of the Luna Network HSM (T-Series). Internal to the Luna Network HSM (T-Series), the module's proprietary command interface (ICD) is used to configure the module's mode of operation.

The module is contained in its own secure enclosure that provides physical resistance to tampering.

Module Type: Hardware

Module Embodiment: MultiChipEmbed

Cryptographic Boundary:

The cryptographic boundary is defined as the entire PCIe card as shown below.

Figure 3 Luna T7 (872-500025-001)

Figure 4 Luna T7U (875-500025-002)

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Luna T-Series Cryptographic Module (T7)	872-500025-001	Firmware: 7.15.1, Bootloader: 2.0.1	NXP C292 PowerPC e500v2 Core-based SoC	Half-height PCIe card with factory installed heatsinks
Luna T-Series Cryptographic Module (T7U)	875-500025-002	Firmware: 7.15.1, Bootloader: 2.0.2	NXP C293 PowerPC e500v2 Core-based SoC	Half-height PCIe card with factory installed heatsinks

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

The Luna T7 excludes the following components from the cryptographic boundary:

- Physical ports
- Cable sockets
- USB host controller
- Power inductors
- Power capacitors
- Step-down switching regulator

2.4 Modes of Operation

The Luna T7 supports the modes of operation listed below.

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	Approved mode	Approved	'The HSM is in FIPS 140-3 approved operation mode'
STM	Secure transport mode, most cryptographic service are not available	Approved	'HSM was successfully configured for transport.'

Table 3: Modes List and Description

Important: the Luna T7 must be configured per section 11.1.2 of this security policy to operate in the modes listed above.

2.5 Algorithms

2.5.1 Approved Algorithms

The following cryptographic library and associated CAVP certificates are used by the cryptographic module:

- **Firmware Cryptographic Library** (A7879);
- **Hybrid (FW/HW) Cryptographic Library** (A7880).

Firmware

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A7879	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A7879	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A7879	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A7879	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A7879	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A7879	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A7879	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
DSA SigVer (FIPS186-4)	A7879	L - 1024, 2048, 3072 N - 160, 224, 256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA KeyGen (FIPS186-5)	A7879	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7879	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A7879	Component - No Curve - 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 Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A7879	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
HMAC-SHA-1	A7879	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A7879	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-256	A7879	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA2-384	A7879	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA2-512	A7879	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
HMAC-SHA3-224	A7879	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA3-256	A7879	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA3-384	A7879	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA3-512	A7879	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A7879	Domain Parameter Generation Methods - P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-IFC-SSC	A7879	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-basic Scheme - KAS2 - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA TwoStep SP800-56Cr2	A7879	MAC Salting Methods - default KDF Mode - counter Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8	SP 800-56C Rev. 2
KDF SP800-108	A7879	KDF Mode - Counter Supported Lengths - Supported Lengths: 128-512 Increment 64	SP 800-108 Rev. 1
KTS-IFC	A7879	Modulo - 4096 Key Generation Methods - rsakpg1-basic Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 512	SP 800-56B Rev. 2
LMS KeyGen	A7879	LMS Modes - LMS_SHA256_M24_H10, LMS_SHA256_M24_H15, LMS_SHA256_M24_H5, LMS_SHA256_M32_H10, LMS_SHA256_M32_H15, LMS_SHA256_M32_H5	SP 800-208
LMS SigGen	A7879	LMS Modes - LMS_SHA256_M24_H10, LMS_SHA256_M24_H15, LMS_SHA256_M24_H5, LMS_SHA256_M32_H10, LMS_SHA256_M32_H15, LMS_SHA256_M32_H5	SP 800-208
LMS SigVer	A7879	LMS Modes - LMS_SHA256_M24_H10, LMS_SHA256_M24_H15, LMS_SHA256_M24_H20, LMS_SHA256_M24_H25, LMS_SHA256_M24_H5, LMS_SHA256_M32_H10, LMS_SHA256_M32_H15, LMS_SHA256_M32_H20, LMS_SHA256_M32_H25, LMS_SHA256_M32_H5	SP 800-208
ML-DSA KeyGen	A7879	Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87	FIPS 204
ML-DSA SigGen	A7879	Deterministic - No, Yes	FIPS 204
ML-DSA SigVer	A7879	-	FIPS 204
ML-KEM EncapDecap	A7879	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768 Functions - Decapsulation, Encapsulation	FIPS 203
ML-KEM KeyGen	A7879	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768	FIPS 203

Algorithm	CAVP Cert	Properties	Reference
PBKDF	A7879	Iteration Count - Iteration Count: 10-1000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-5)	A7879	Key Generation Mode - probable, probableWithProbableAux Hash Algorithm - SHA2-256 Modulo - 2048, 3072, 4096 Primality Tests - 2pow100 Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A7879	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A7879	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A7879	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1	A7879	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-224	A7879	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	A7879	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	A7879	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4
SHA2-512	A7879	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4
SHA3-224	A7879	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-256	A7879	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-384	A7879	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-512	A7879	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHAKE-128	A7879	-	FIPS 202
SHAKE-256	A7879	-	FIPS 202
TDES-CBC	A7879	Direction - Decrypt	SP 800-67 Rev. 2

Table 4: Approved Algorithms - Firmware

Hybrid

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A7880	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A7880	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A7880	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A7880	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A7880	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
DSA SigVer (FIPS186-4)	A7880	L - 1024, 2048, 3072 N - 160, 224, 256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA KeyGen (FIPS186-5)	A7880	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7880	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A7880	Component - No Curve - 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 Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A7880	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
Hash DRBG	A7880	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA-1	A7880	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A7880	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA2-256	A7880	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA2-384	A7880	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA2-512	A7880	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
HMAC-SHA3-224	A7880	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-256	A7880	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA3-384	A7880	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA3-512	A7880	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A7880	Domain Parameter Generation Methods - P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-IFC-SSC	A7880	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-basic Scheme - KAS2 - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA TwoStep SP800-56Cr2	A7880	MAC Salting Methods - default KDF Mode - counter Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8	SP 800-56C Rev. 2
KDF SP800-108	A7880	KDF Mode - Counter Supported Lengths - Supported Lengths: 128-512 Increment 64	SP 800-108 Rev. 1
KTS-IFC	A7880	Modulo - 4096 Key Generation Methods - rsakpg1-basic Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 512	SP 800-56B Rev. 2
LMS KeyGen	A7880	LMS Modes - LMS_SHA256_M24_H10, LMS_SHA256_M24_H15, LMS_SHA256_M24_H5, LMS_SHA256_M32_H10, LMS_SHA256_M32_H15, LMS_SHA256_M32_H5	SP 800-208
LMS SigGen	A7880	LMS Modes - LMS_SHA256_M24_H10, LMS_SHA256_M24_H15, LMS_SHA256_M24_H5, LMS_SHA256_M32_H10, LMS_SHA256_M32_H15, LMS_SHA256_M32_H5	SP 800-208
LMS SigVer	A7880	LMS Modes - LMS_SHA256_M24_H10, LMS_SHA256_M24_H15, LMS_SHA256_M24_H20, LMS_SHA256_M24_H25, LMS_SHA256_M24_H5, LMS_SHA256_M32_H10, LMS_SHA256_M32_H15, LMS_SHA256_M32_H20, LMS_SHA256_M32_H25, LMS_SHA256_M32_H5	SP 800-208
ML-DSA KeyGen	A7880	Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87	FIPS 204
ML-DSA SigGen	A7880	Deterministic - No, Yes	FIPS 204
ML-DSA SigVer	A7880	-	FIPS 204
ML-KEM EncapDecap	A7880	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768 Functions - Decapsulation, Encapsulation	FIPS 203
ML-KEM KeyGen	A7880	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768	FIPS 203
PBKDF	A7880	Iteration Count - Iteration Count: 10-1000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-5)	A7880	Key Generation Mode - probable, probableWithProbableAux Hash Algorithm - SHA2-256	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		Modulo - 2048, 3072, 4096 Primality Tests - 2pow100 Private Key Format - standard	
RSA SigGen (FIPS186-5)	A7880	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A7880	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A7880	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1	A7880	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-224	A7880	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	A7880	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	A7880	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4
SHA2-512	A7880	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4
SHA3-224	A7880	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-256	A7880	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-384	A7880	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-512	A7880	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
TDES-CBC	A7880	Direction - Decrypt	SP 800-67 Rev. 2

Table 5: Approved Algorithms - Hybrid

2.5.2 Vendor-Affirmed Algorithms

Name	Properties	Implementation	Reference
CKG	Key type:Symmetric	Luna T7 Firmware Cryptographic Library	SP 800-133r2, Section 4

Table 6: Vendor-Affirmed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Authenticated Symmetric Encryption/Decryption	BC-Auth	Block Cipher, Authenticated		AES-GCM: (A7880)
Cryptographic Message Authentication	MAC	Message Authentication		AES-CMAC: (A7879, A7880) AES-GMAC: (A7880)
DSA Signature Verification	DigSig-SigVer	Signature Verification, DSA		DSA SigVer (FIPS186-4): (A7879, A7880) SHA-1: (A7879, A7880) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880)
ECDSA Key Generation	AsymKeyPair-KeyGen	Asymmetric key pair generation, ECDSA		ECDSA KeyGen (FIPS186-5): (A7879, A7880)
ECDSA Signature Generation	DigSig-SigGen	Signature Generation, ECDSA		ECDSA SigGen (FIPS186-5): (A7879, A7880) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880) SHA3-224: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-384: (A7879, A7880) SHA3-512: (A7879, A7880)
ECDSA Signature Verification	DigSig-SigVer	Signature Verification, ECDSA		ECDSA SigVer (FIPS186-4): (A7879, A7880) ECDSA SigVer (FIPS186-5): (A7879, A7880) SHA-1: (A7879, A7880) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880) SHA3-224: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-384: (A7879, A7880) SHA3-512: (A7879, A7880)
Generate Entropy	ENT-ESV	Generate random data used as seed for Generate Random Data.		
Generate Random Data	DRBG	Deterministic random bit generator		Hash DRBG: (A7880) SHA2-256: (A7880)

Name	Type	Description	Properties	Algorithms
Hash Message Authentication	MAC	Message Authentication		HMAC-SHA-1: (A7879, A7880) HMAC-SHA2-224: (A7879, A7880) HMAC-SHA2-256: (A7879, A7880) HMAC-SHA2-384: (A7879, A7880) HMAC-SHA2-512: (A7879, A7880) HMAC-SHA3-224: (A7879, A7880) HMAC-SHA3-256: (A7879, A7880) HMAC-SHA3-384: (A7879, A7880) HMAC-SHA3-512: (A7879, A7880)
KAS-ECC	KAS-Full	ECC Key Agreement	IG D.F:Scenario 2 path 2 Key confirmation:No Key derivation:KDA Caveat:Provides 192 bits of security strength	ECDSA KeyGen (FIPS186-5): (A7879, A7880) KAS-ECC-SSC Sp800-56Ar3: (A7879, A7880) KDA TwoStep SP800-56Cr2: (A7879, A7880) AES-CMAC: (A7879, A7880)
KAS-RSA	KAS-Full	RSA Key Agreement	IG D.F:Scenario 1 path 2 Key confirmation:No Key derivation:KDA Caveat:Provides 128 or 192 bits of security strength	RSA KeyGen (FIPS186-5): (A7879, A7880) KAS-IFC-SSC: (A7879, A7880) KDA TwoStep SP800-56Cr2: (A7879, A7880) SHA2-512: (A7879, A7880) AES-CMAC: (A7879, A7880)
KEM Decaps	KEM-Decap	Decapsulate and derive shared secret key	IG D.S:Scenario 1	ML-KEM EncapDecap: (A7879, A7880) Function: Decapsulate SHA3-256: (A7879, A7880) SHA3-512: (A7879, A7880) SHAKE-128: (A7879) SHAKE-256: (A7879)
KEM Encaps	KEM-Encap	Derive and encapsulate shared secret	IG D.S:Scenario 1	ML-KEM EncapDecap: (A7879, A7880) Function: Encapsulate

Name	Type	Description	Properties	Algorithms
				SHA3-256: (A7879, A7880) SHA3-512: (A7879, A7880) SHAKE-128: (A7879) SHAKE-256: (A7879)
KEM KeyGen	AsymKeyPair-KeyGen	Generate ML-KEM public/private key pair		ML-KEM KeyGen: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-512: (A7879, A7880) SHAKE-128: (A7879)
KTS-AES	KTS-Wrap	Wraps / Unwraps key data	IG D.G:Approved method Caveat:Provides 128, 192 or 256 bits of security strength	AES-KW: (A7880) AES-KWP: (A7880)
KTS-HMAC	KTS-Wrap	Wraps/Unwraps key data, HMAC Authenticated	IG D.G:Approved method Caveat:Provides 256 bits of security strength	AES-CBC: (A7879, A7880) HMAC-SHA2-256: (A7879, A7880)
KTS-RSA	KTS-Decap PBKDF	Decrypts received authentication data when using password authentication	IG D.G:Approved method Key confirmation:No Caveat:Provides 128 bits of security strength	KTS-IFC: (A7879, A7880) PBKDF: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-512: (A7879, A7880)
Key-Based KDF	KBKDF	Key Based Key Derivation		KDF SP800-108: (A7879, A7880) AES-CMAC: (A7879, A7880) HMAC-SHA2-224: (A7879, A7880) HMAC-SHA2-256: (A7879, A7880) HMAC-SHA2-384: (A7879, A7880) HMAC-SHA2-512: (A7879, A7880) HMAC-SHA3-224: (A7879, A7880) HMAC-SHA3-256: (A7879, A7880) HMAC-SHA3-384: (A7879, A7880) HMAC-SHA3-512: (A7879, A7880)
LMS Key Pair Generation	AsymKeyPair-KeyGen	Key generation, LMS		LMS KeyGen: (A7879, A7880) SHA2-256: (A7879, A7880)

Name	Type	Description	Properties	Algorithms
LMS Signature Generation	DigSig-SigGen	Signature Generation, LMS		LMS SigGen: (A7879, A7880) SHA2-256: (A7879, A7880)
LMS Signature Verification	DigSig-SigVer	Signature Verification, LMS		LMS SigVer: (A7879, A7880) SHA2-256: (A7879, A7880)
Login with PED key	BC-UnAuthDecrypt MAC	Login with PED key		AES-CBC: (A7879, A7880) HMAC-SHA2-256: (A7879, A7880) SHA2-256: (A7879, A7880)
ML-DSA Key Generation	AsymKeyPair-KeyGen	Generate public/private key pair		ML-DSA KeyGen: (A7879, A7880) SHAKE-128: (A7879) SHAKE-256: (A7879)
ML-DSA PreHasSigVer	DigSig-SigVer	Verify signature of data using public key		ML-DSA SigVer: (A7879, A7880) SHAKE-128: (A7879) SHAKE-256: (A7879) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880) SHA3-224: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-384: (A7879, A7880) SHA3-512: (A7879, A7880)
ML-DSA PreHashSigGen	DigSig-SigGen	Generate a signature of data using private key		ML-DSA SigGen: (A7879, A7880) SHAKE-128: (A7879) SHAKE-256: (A7879) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880) SHA3-224: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-384: (A7879, A7880) SHA3-512: (A7879, A7880)
ML-DSA PureSigGen	DigSig-SigGen	Generate a signature of data using private key		ML-DSA SigGen: (A7879, A7880) SHAKE-128: (A7879) SHAKE-256: (A7879)
ML-DSA PureSigVer	DigSig-SigVer	Verify signature of data using public key		ML-DSA SigVer: (A7879, A7880)

Name	Type	Description	Properties	Algorithms
				SHAKE-128: (A7879) SHAKE-256: (A7879)
RSA Key Pair Generation	AsymKeyPair-KeyGen	Asymmetric key pair generation, RSA		RSA KeyGen (FIPS186-5): (A7879, A7880) SHA2-256: (A7879, A7880)
RSA Signature Generation	DigSig-SigGen	Signature Generation, RSA		RSA SigGen (FIPS186-5): (A7879, A7880) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880) SHA3-224: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-384: (A7879, A7880) SHA3-512: (A7879, A7880)
RSA Signature Verification	DigSig-SigVer	Signature Verification, RSA		RSA SigVer (FIPS186-4): (A7879, A7880) RSA SigVer (FIPS186-5): (A7879, A7880) SHA-1: (A7879, A7880) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880) SHA3-224: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-384: (A7879, A7880) SHA3-512: (A7879, A7880)
Secure Hash	SHA	Secure Hash		SHA-1: (A7879, A7880) SHA2-224: (A7879, A7880) SHA2-256: (A7879, A7880) SHA2-384: (A7879, A7880) SHA2-512: (A7879, A7880) SHA3-224: (A7879, A7880) SHA3-256: (A7879, A7880) SHA3-384: (A7879, A7880) SHA3-512: (A7879, A7880)
Symmetric Encryption/Decryption	BC-UnAuth	Block Cipher, Unauthenticated		AES-CBC: (A7879, A7880) AES-CFB128: (A7879, A7880) AES-CFB8: (A7879, A7880) AES-CTR: (A7879, A7880) AES-ECB: (A7879, A7880)

Name	Type	Description	Properties	Algorithms
				AES-OFB: (A7879, A7880) AES-XTS Testing Revision 2.0: (A7880) TDES-CBC: (A7879, A7880)
Symmetric Key Generation	CKG	Generation of symmetric keys and seeds for asymmetric keys		CKG: () Key type: Symmetric
Two-Step KDF	KAS-56CKDF	Two-step key derivation		KDA TwoStep SP800-56Cr2: (A7879, A7880) AES-CMAC: (A7879, A7880)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES-GCM IV Generation

The module's AES-GCM implementation conforms to IG:C.H Scenario 2. The IV is generated internally by the module using approved Hash_DRBG (SHA2-256). The IV generation supported is fixed 96-bit size that is generated with the SP800 90A Hash_DRBG (SHA2-256) output.

2.7.2 PBKDF

Password Length and Probability – Refer to Section 4.1 for a description of the minimum password length and the upper bound of the probability of having this parameter guessed at random.

Iteration Count and Justification – The PBKDF is only used for internal operations, with a SP800-132 compliant iteration count fixed at a value of 1000. Larger iteration counts were measured to take as long as 5 minutes to derive the key.

Storage Only Statement – PBKDF, used when configured to use Password Authentication, is used to derive a key, from a user's password. The module uses method 1a from SP800-132 where the derived key is used to protect the data. The data protected is the user's user storage key (USK).

2.7.3 XTS-AES

XTS-AES may only be used for storage applications.

For XTS-AES keys that are entered into the module, the operator must ensure that the two halves of the key (payload and tweak) have been generated and/or established independently of each other, according to the rules for component symmetric keys from NIST SP 800-133rev2, section 6.3.

For XTS-AES keys generated by the module, this independence requirement is implicitly met.

2.8 RBG and Entropy

The Luna T7 contains two separate and distinct entropy sources. A module policy configuration under the control of the Security Officer determines which entropy source is used to Instantiate and Reseed the DRBG.

Cert Number	Vendor Name
E252	Thales
E63	ID Quantique SA

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
IDQ Quantis IID QRNG	Physical	IDQ6MC1	2048	1792	N/A
Thales Luna T7 Entropy Source	Physical	NXP C29X SoC	384	332.69	N/A

Table 9: Entropy Sources

2.8.1 Thales Luna T7 Entropy Source

The Thales Luna T7 Entropy Source is a physical entropy source based on a ring oscillator. It is contained within the NXP PowerPC SoC (System-On-Chip) - the CPU of the Luna T7.

To generate entropy, this source generate blocks of 2500 1-bit noise samples. These are subjected to 15 statistical tests. For blocks that pass these tests, the first 384 bits are inserted into the entropy buffer. The remainder are discarded.

2.8.2 IDQ Quantis IID QRNG

The IDQ Quantis IID QRNG is a physical entropy source based on photon source and CMOS sensor. This source is provided as alternative should the operator require a quantum-based entropy source.

To generate entropy, the source generates a 2048-bit block comprised of 1024 2-bit noise samples. These are subjected to the RCT and APT health tests (described in section 10.2 below). For blocks that pass these tests, the entire block is inserted into the entropy buffer.

2.8.3 Entropy buffer

The module maintains a 2048-bit entropy buffer. This buffer is drawn down by the seeding and reseeding of the DRBG. When empty, the buffer is replenished from the selected entropy source.

2.8.4 DRBG Seeding and reseeding

The module's DRBG is hosted in the NXP PowerPC SoC. To initially seed the DRBG, 640 bits are drawn from the entropy buffer. If the Luna T7 (NXP) entropy source is being used, this seed will contain 554 bits of entropy. If using the IDQ source, the seed will contain 560 bits of entropy.

During reseeding, 512 bits are drawn from the entropy buffer. If the Luna T7 (NXP) entropy source is being used, this seed will contain 443 bits of entropy. If using the IDQ source, the seed will contain 448 bits of entropy.

These both exceed the 440 bits required to instantiate or reseed the entropy source to a security strength of 256 bits.

2.8.5 RBG Output

The output of the DRBG is used for Generate Random Data and for Symmetric Key Generation SFIs.

2.9 Key Generation

In accordance with FIPS 140-3 Implementation Guidance (IG) D.H, the cryptographic module performs Cryptographic Key Generation (CKG) in compliance with section 4 of SP 800-133r2. Symmetric cryptographic keys are generated by the direct unmodified output of the module’s approved DRBG. The DRBG output is also used as a seed for asymmetric key generation.

User passwords for authentication are provided by the operator. PED key authentication data is generated by the module.

2.10 Key Establishment

2.10.1 Key Import and Export

The ICD communication path to the host is used for entry/output of: certificates, user password and Secure Audit Logging Key (SALK).

If the module has been configured to use the PED, the direct connection to the PED is used for entry/output of: PED Authentication Data, Cloning Domain Vector/Key Cloning Vector (KCV), Remote PED Vector (RPV), and Secure Recovery Vector (SRV).

The remaining keys and SSPs 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:

2.10.2 Key Cloning

Key cloning uses, the Cloning Key Encryption Vector (CKEV), to wrap, using KWP, objects transferred from one cryptographic module to another. Objects transferred using the cloning protocol may be keys, user data, or module data. The CKEV is only valid for the Key Cloning session.

The key derivation method is a Two-Step Key Derivation Function with Randomness Extraction per SP800-56Cr2 and SP800-108. FixedInfo consists of the concatenated KCV, the target's TWC length and TWC and the source's TWC length and TWC.

2.10.3 Key Transport

The module implements the following approved key transport methods (per 140-3 IG D.G):

- Using AES-KW and AES-KWP compliant to SP 800-38F - providing between 128 and 256 bits of encryption strength
- Using RSA-OAEP compliant to SP 800-56Brev2 - providing 128 bits of encryption strength
- Using AES-CBC and HMAC-SHA2-256 compliant to SP 800-38A and FIPS 198 - providing 256 bits of encryption strength

2.10.4 Key Agreement

The module implements the following approved key agreement methods (per 140-3 IG D.F):

Establishing an EC DH shared secret compliant to SP 800-56Arev3 - providing 192 bits of encryption strength based on the support of only the P-384 curve

Establishing an IFC shared secret compliant to SP 800-56Brev2 - providing 128 to 192 bits of encryption strength based on the modulus sizes supported

2.10.5 Key establishment mechanisms

The module does not establish SSPs using an approved key encapsulation mechanism (KEM). However, it does offer some or all of the underlying KEM cryptographic functionality to be used by an external operator/application as part of an approved KEM.

2.11 Industry Protocols

The module does not claim to support any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCIe	Data Input Data Output Control Input Status Output	Cryptographic data, keys, authentication data, ICD commands
USB Host	Data Input Data Output	Cryptographic data, keys, authentication data
Serial PED	Data Input Data Output	Authentication data
External Event (Tamper)	Control Input	External Event Alarm
Decommission	Control Input	Decommission Alarm
LED	Status Output	System status
Power	Power	12V main supply to generate internal module supply rails and USB Host port 5V power
Battery	Power	3.6V battery supply

Table 10: Ports and Interfaces

The following figures (Figure 5 and Figure 6) show the location of the physical ports of the cryptographic module:

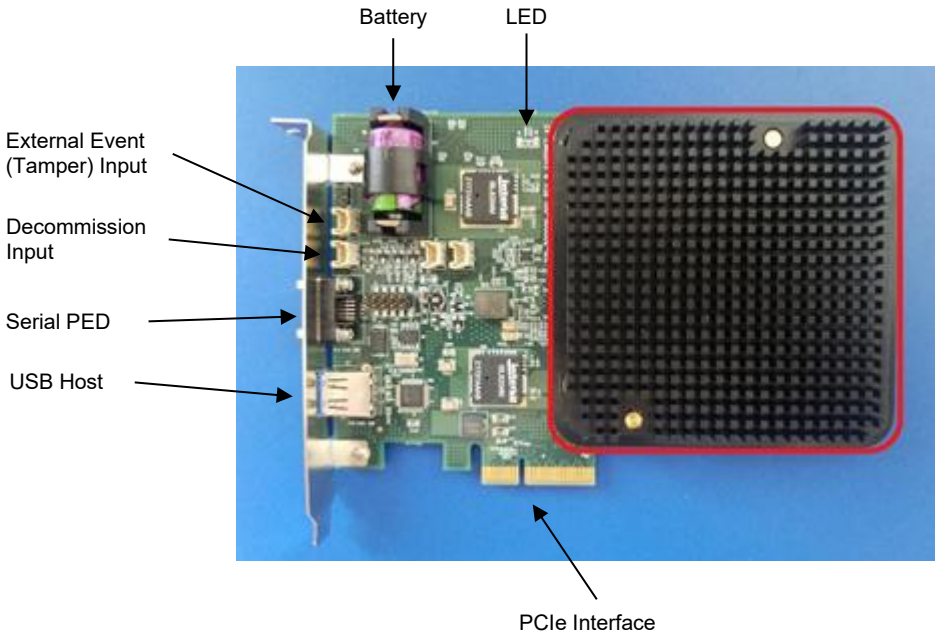

Figure 5 Luna T7 Physical Ports

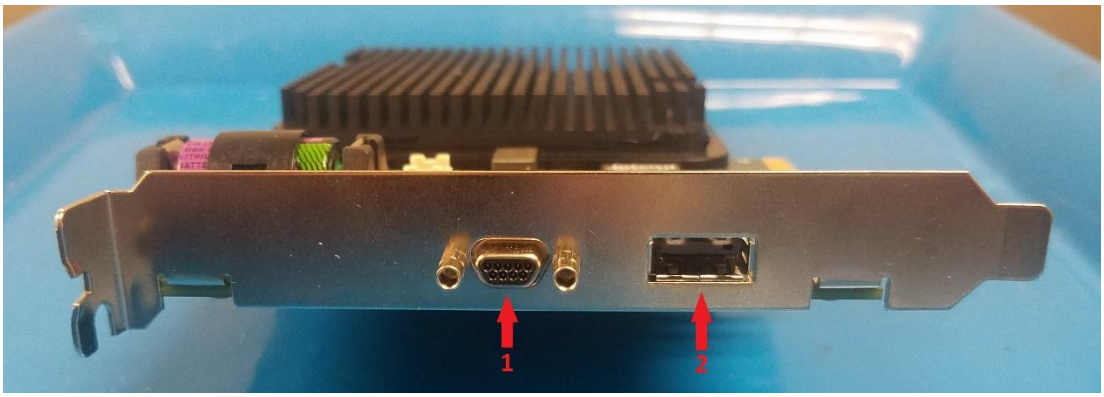

Figure 6 Luna T7 PCI Bracket View

In Figure 6. 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.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
MFA	48-byte random authentication data plus 16-byte Challenge Secret generated when a role is initialized and stored on PED Key.	Login with PED key	1 in 10^115	1 in 10^114
PED Key	48-byte random authentication data generated when a role is initialized and stored on PED Key.	Login with PED key	1 in 10^115	1 in 10^114
Password	User provided byte array (minimum 8 bytes).	KTS-RSA	1 in 10^19	1 in 10^18

Table 11: Authentication Methods

The authentication objective is to ensure that only authorized users or applications can:

- manage or supervise the module
- access cryptographic functions of the module
- access sensitive cryptographic keys stored within the module

The strength of the available authentication mechanisms shall conform to the following:

- For each attempt to use the authentication mechanism, the probability shall be less than 1 in 1,000,000 that a random attempt will succeed or a false acceptance will occur.
- For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than 1 in 100,000 that a random attempt will succeed or a false acceptance will occur.

The Luna T7 can be configured for either Password-based or PED-based authentication. The default setting is Password-based authentication. A user with proper authority can change the authentication method between Password and PED.

All roles except for the Public User must authenticate to the module by providing their authentication data. The table above explains the type and strength of the authentication supported for each role.

If configured to use PED authentication, all roles must authenticate using a PED Key. When a role is initialized under this configuration, the module generates the authentication data as a 48-byte random value and writes it to a PED Key. The PED key is used to authenticate the user.

In addition to providing PED Key, the Crypto User, in order to authenticate, must also provide a Challenge Secret. The Challenge Secret is a random number generated by the module and displayed on the PED when creating the user. It is a memorized secret shared between the user and the module. To authenticate, the user provides the PED Key and enters, on the PED, the Challenge Secret.

The Challenge Secret is an option for the Crypto Officer.

Figure 7 shows the PIN Entry Device (PED), with PED Keys, used for PED-authentication.

Figure 7 PIN Entry Device (PED) and PED Keys

If configured to use Password authentication, 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 Approved mode, the password is delivered to the module encrypted with the module's Password Encryption Certificate (PEC) using an RSA-OAEP and a random nonce to prevent replay attacks.

For Password Authentication, the PIN Storage Key (PSK) is derived from the delivered password using SP800-132 PBKDF. For PED Authentication, the PSK is delivered from the PED. The PSK is used to uncover the encrypted partition authentication data (i.e. checkword). If the decrypted checkword is valid, the user role is authenticated; otherwise, a login error is returned and logged.

4.1.1 Identity

NOTE: All methods of authentication supported by the module (memorized secret or multi-factor PED key + memorized secret), incorporate the use of an ID alongside the presentation of the authentication data and are identity-based.

4.1.2 Activation

If the module is configured to use PED authentication, the Crypto Officer and Crypto User 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 Challenge Secret password.

Once activated, it remains activated until explicitly deactivated, deleted or the module is reset.

4.1.3 M of N

If the module is configured to use PED authentication, 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 different 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 randomly generated authentication data.

4.1.4 PED Keys

If configured, the Luna T7 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 path. CSPs and authentication data that are output to the Luna PED are stored in PED Keys. A PED Key is a USB device connected to the Luna PED.

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 (CU) PED Key – for the storage of Cryptographic Officer (Partition Owner) authentication data
- Gray (CU) PED Key – for the storage of Cryptographic User (Partition 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

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Audit Officer (AO)	Identity	Crypto Officer	Password PED Key
Crypto Officer (CO)	Identity	User	Password PED Key MFA
Crypto User (CU)	Identity	User	Password MFA
HSM Security Officer (SO)	Identity	Crypto Officer	Password PED Key

Table 12: Roles

4.3 Approved Services

The services listed here use Security Function Implementations listed in Section 2.6.

The SSP Access column, for each approved service, lists the SSPs used by and how the service uses the SSP. The following is the key for how the service uses the SSP:

- G = Generate: The service generates or derives the SSP;
- R = Read: The service outputs the SSP (e.g. read from the module);
- W = Write: The service imports the SSP (e.g. written to the module);
- E = Execute: The service uses the SSP in performing a cryptographic operation; and
- Z = Zeroize: The service zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Audit Config	Configure the audit log and mechanism	Implicit	Session, log configuration parameter and value	-	Hash Message Authentication	Audit Officer (AO) - SALK: E
Audit Log Secret Export	Wrap and export the SALK.	Implicit	Session	Wrapped log secret	KTS-AES Two-Step KDF	Audit Officer (AO) - KCV: E - SADK: G,E - SALK: R - U2K: E
Audit Log Secret Import	Import and unwrap the SALK.	Implicit	Session, wrapped log secret	-	KTS-AES Two-Step KDF	Audit Officer (AO) - KCV: E - SADK: E - SALK: W - U2K: E
Audit Log Verify	Checks the authenticity of extracted sections of the audit log.	Implicit	Command	-	Hash Message Authentication	HSM Security Officer (SO) - SALK: E Audit Officer (AO) - SALK: E
Audit Role Init	Create the Audit Officer role	Implicit	AO Auth Data (Pwd Auth), Domain	AO Auth Data (PED Auth)	Generate Random Data KTS-HMAC KTS-RSA	Unauthenticated - PED Key Authentication Data: R,W,E - User Password: W,E - GSK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KCV: G,E - PEC: R - PSK: G,E - RDEK: E - RMAC: E - RPV: E - USK: G,E - DRBG output: G
Cloning Tunnel	Establishes a secure connection to another module (Cannot be invoked by operator, automatically invoked by module when cloning service is invoked)	Implicit	-	-	Generate Random Data KAS-RSA	HSM Security Officer (SO) - RSA Shared secret: G - TWC: R,W,E - KCV: E - CKEV: G Crypto Officer (CO) - RSA Shared secret: G - TWC: R,W,E - KCV: E - CKEV: G
Configuration Update	Verify the signature of a configuration update file	Implicit	Session, CUF (Signed Configuration Update File)	-	RSA Signature Verification	HSM Security Officer (SO) - LSC: W - ROOT: E
Crypto User Role Init	Creates the Crypto User role on a partition	Implicit	Session	Challenge Secret	Generate Random Data KTS-HMAC	Crypto Officer (CO) - Challenge Secret: G,R - RDEK: E - RMAC: E - RPV: E - SGSK: E - DRBG output: G Crypto User (CU) - Challenge Secret: G,R - RDEK: E - RMAC: E - RPV: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SGSK: E - DRBG output: G
Delete key	Delete a key in a user's partition	-	Session, key handle	-	None	HSM Security Officer (SO) - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z Crypto Officer (CO) - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
Derive Key	Derive new keys from existing keys on a user's partition.	Implicit	Session, algorithm, algorithm parameters, derivation key handles	Derived key handle	Symmetric Encryption/Decryption Key-Based KDF KEM Encaps KEM Decaps	HSM Security Officer (SO) - MTK: E - SMK: E - Partition Symmetric Key: G,E - Partition ML-KEM Public Key: E - Partition ML-KEM Private Key: E Crypto Officer (CO) - MTK: E - USK: E - Partition Symmetric Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E - Partition ML-KEM Public Key: E - Partition ML-KEM Private Key: E
Enable / Disable STM	Enables or disables Secure Transport Mode functionality	-	Session, SRV (disable)	SRV (enable)	None	HSM Security Officer (SO) - RPV: E - SRV: R,W - DRBG output: E
Enter STM	Enters Secure Transport mode	Implicit	-	SRV	KTS-HMAC	Unauthenticated - MTK: Z - RDEK: E - RMAC: E - RPV: E - SRV: R - DRBG output: E
Exit STM	Exits Secure Transport mode	Implicit	SRV	-	KTS-HMAC	Unauthenticated - MTK: G - RDEK: E - RMAC: E - RPV: E - SRV: W
Firmware Update	Verify then load a new firmware image	Implicit	Session, FUF (Signed Firmware Update File)	-	RSA Signature Verification	HSM Security Officer (SO) - FSC: W - GSK: E - ROOT: E - U2K: E
Generate Key	Generate keys or key pairs on user's partition.	Implicit	Session, generation algorithm, algorithm parameter, key attributes	Key handles	Generate Random Data Symmetric Key Generation RSA Key Pair Generation ECDSA Key Generation LMS Key Pair Generation ML-DSA Key	HSM Security Officer (SO) - MTK: E - SMK: E - Partition Symmetric Key: G - Partition ECDSA Public Key: G - Partition ECDSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Generation KEM KeyGen	Key: G - Partition LMS Private Key: G - Partition RSA Public Key: G - Partition RSA Private Key: G - DRBG output: E - Partition ML-DSA Public Key: G - Partition ML-DSA Private Key: G - Partition ML-KEM Public Key: G - Partition ML-KEM Private Key: G Crypto Officer (CO) - MTK: E - USK: E - Partition Symmetric Key: G - Partition ECDSA Public Key: G - Partition ECDSA Private Key: G - Partition LMS Private Key: G - Partition RSA Public Key: G - Partition RSA Private Key: G - DRBG output: E - Partition ML-DSA Public Key: G - Partition ML-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DSA Private Key: G - Partition ML-KEM Public Key: G - Partition ML-KEM Private Key: G
Generate Random Data	Generate a random number from the DRBG	Implicit	Request size	Requested random data	Generate Random Data	Unauthenticated - DRBG_C: E - DRBG_V: E - DRBG output: G
HSM Initialize	This service is used to initialize the HSM on first use or following zeroization. Actions performed by this service include: - resets the admin partition; - deletes all user partitions; - generates the KEK; - initializes the HSM SO role; - creates / selects KCV to be used with the admin partition; - generates PEC, PEK, and SMK keys for the admin partition; and - encrypts keys for storage	Implicit	SO Authentication data, Cloning Domain	SO Auth data (PED Auth)	Generate Random Data RSA Key Pair Generation RSA Signature Generation KTS-RSA KTS-HMAC	Unauthenticated - PED Key Authentication Data: R,W,E - User Password: W,E - CITS-DAK: G - CITS-DAC: G - GSK: E - HOK: E - KCV: G,R,W,Z - KEK: G,E - PEK: G,E - PEC: G,R - PSK: G,E - RDEK: E - RMAC: E - RPV: G,R,E - SGSK: G,E - SMK: G,W,E - TUK: G - TVK: Z - TWC: G - USK: Z - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
HSM Set Policy	Set HSM policy.	-	Session, HSM Policy Number, Value	-	None	HSM Security Officer (SO) - Challenge Secret: Z - GSK: Z - KCV: Z - SGSK: Z - USK: Z - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
Hash Digest	Generate a hash over a block of supplied data.	Implicit	Session, algorithm, data to hash	Hash digest	Secure Hash	Unauthenticated
Import Public Key	Import objects into a user partition.	Implicit	Public key, certificate, domain objects, data objects	Imported object handle	KTS-AES	HSM Security Officer (SO) - Partition DSA Public Key: W - Partition ECDSA Public Key: W - Partition LMS Public Key: W - Partition RSA Public Key: W - Partition ML-DSA Public Key: W - Partition ML-KEM Public Key: W Crypto Officer (CO) - Partition DSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: W - Partition ECDSA Public Key: W - Partition LMS Public Key: W - Partition RSA Public Key: W - Partition ML-DSA Public Key: W - Partition ML-KEM Public Key: W
Initialize Remote PED Vector	Creates the Remote PED Vector (RPV). Stores the RPV locally in HSM Flash and remotely on the RPV PED Key device.	Implicit	Session, RPV PED Index	Remote PED Vector	Generate Random Data	HSM Security Officer (SO) - DRBG output: E - RPV: G,R,W Crypto Officer (CO) - DRBG output: E - RPV: G,R,W
Key export	Export user partition secret or private key objects	Implicit	Session, wrapping key handle, key to wrap handle	Wrapped key blob	Symmetric Encryption/Decryption KTS-AES	HSM Security Officer (SO) - MTK: E - SMK: E - Partition Symmetric Key: R - Partition ECDSA Private Key: R - Partition RSA Private Key: R - Partition ML-DSA Private Key: R - Partition ML-KEM Private Key: R Crypto Officer (CO) - MTK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- USK: E - Partition Symmetric Key: R - Partition ECDSA Private Key: R - Partition RSA Private Key: R - Partition ML-DSA Private Key: R - Partition ML-KEM Private Key: R
Key import	Import user partition secret or private key objects.	Implicit	Session, wrapping key handle,, wrapped key blob, key attributes	Unwrapped key handle	KTS-AES	HSM Security Officer (SO) - MTK: E - SMK: E - Partition Symmetric Key: W - Partition ECDSA Private Key: W - Partition RSA Private Key: W - Partition ML-DSA Private Key: W - Partition ML-KEM Private Key: W Crypto Officer (CO) - MTK: E - USK: E - Partition Symmetric Key: W - Partition ECDSA Private Key: W - Partition RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: W - Partition ML-DSA Private Key: W - Partition ML-KEM Private Key: W
Login using MFA	Login to the module using multi-factor authentication. If an SO Login fails and exceeds the threshold count, a SO zeroization occurs. If a CO Login fails and exceeds the threshold count, a CO zeroization occurs	Implicit	Role PED Auth Data, Challenge Response	Random Challenge, response	Generate Random Data Login with PED key	Unauthenticated - Challenge Response: W,Z - PED Key Authentication Data: W,E - CITS-DAK: G - CITS-DAC: G - GSK: E,Z - HOK: E - KCV: G,E,Z - PEK: G,E - PEC: G,R - PSK: G,E - RDEK: E - RMAC: E - RPV: E - SGSK: G,E,Z - SMK: E,Z - TUK: G - TWC: G - TVK: Z - USK: E,Z - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Random Challenge: R - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
Login using PED key	Login to the module using PIN entry device	Implicit	Role PED Auth Data, Challenge Response	Random Challenge, response	Generate Random Data KTS-HMAC Login with PED key	Unauthenticated - PED Key Authentication Data: W,E - CITS-DAK: G - CITS-DAC: G - GSK: E,Z - HOK: E - KCV: G,E,Z - PEK: G,E - PEC: G,R - PSK: G,E - RDEK: E - RMAC: E - SGSK: G,E,Z - TUK: G - TWC: G - SMK: E,Z - RPV: E - TVK: Z - USK: E,Z - Partition Symmetric Key: Z - Partition DSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Challenge Response: W - Random Challenge: R - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
Login with password	Login to the module using a password	Implicit	Role, password	-	Generate Random Data KTS-RSA	Unauthenticated - User Password: W,E - CITS-DAK: G - CITS-DAC: G - GSK: E,Z - HOK: E - KCV: G,E,Z - PEK: G,E - PEC: G,R - PSK: G,E - RPV: E - SGSK: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SMK: E,Z - TUK: G - TWC: G - TVK: Z - USK: E,Z - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
Logout	Log out of the module	-	Session	-	None	HSM Security Officer (SO) Audit Officer (AO) Crypto Officer (CO) - Partition Symmetric Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z Crypto User (CU) - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
MAC Gen	Generate a MAC over a block of user supplied data.	Implicit	Session, algorithm, algorithm parameter, data to sign	MAC	Symmetric Encryption/Decryption Cryptographic Message Authentication	HSM Security Officer (SO) - MTK: E - SMK: E - Partition Symmetric Key: E Crypto Officer (CO) - MTK: E - USK: E - Partition Symmetric Key: E Crypto User (CU) - MTK: E - USK: E - Partition Symmetric Key: E
MAC Ver	Verify a MAC over a block of user-supplied data.	Implicit	Session, algorithm, algorithm parameter, data to verify	Ruling	Symmetric Encryption/Decryption Cryptographic Message Authentication	HSM Security Officer (SO) - SMK: E - Partition Symmetric Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Crypto Officer (CO) - USK: E - Partition Symmetric Key: E Crypto User (CU) - USK: E - Partition Symmetric Key: E
PED Tunnel	Establishes a secure connection to a local or remote PED (Cannot be invoked by operator, automatically invoked by module when initialization or login services invoked)	Implicit	-	-	Generate Random Data KAS-ECC	Unauthenticated - EC Private key: G,E - EC Public key: G,R - EC Peer public key: W,E - EC Shared secret: G - RDEK: G - RMAC: G - DRBG output: G
Partition Backup / Restore (Clone)	This service exports (Backup) or imports (Restore) data objects for a Crypto Officer partition as part of the Cloning protocol.	Implicit	Session, object handle (Backup), wrapped key object (Restore)	Object handle (Restore), wrapped key object Backup)	RSA Signature Verification KTS-AES	HSM Security Officer (SO) - CKEV: E - HOC: E - KCV: E - MTK: E - MIC: E - ROOT: E - TUK: E - USK: E - Partition Symmetric Key: R,W - Partition DSA Public Key: R,W - Partition ECDSA Public Key: R,W - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Private Key: R,W - Partition LMS Public Key: R,W - Partition RSA Public Key: R,W - Partition RSA Private Key: R,W - DRBG output: E - RSA Shared secret: G - Partition ML-DSA Public Key: R,W - Partition ML-DSA Private Key: R,W - Partition ML-KEM Public Key: R,W - Partition ML-KEM Private Key: R,W Crypto Officer (CO) - CKEV: E - HOC: E - KCV: E - MIC: E - MTK: E - ROOT: E - TUK: E - USK: E - Partition Symmetric Key: R,W - Partition DSA Public Key: R,W - Partition ECDSA Public Key: R,W - Partition ECDSA Private Key: R,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition LMS Public Key: R,W - Partition RSA Public Key: R,W - Partition RSA Private Key: R,W - DRBG output: E - RSA Shared secret: G - Partition ML-DSA Public Key: R,W - Partition ML-DSA Private Key: R,W - Partition ML-KEM Public Key: R,W - Partition ML-KEM Private Key: R,W
Partition Set Policy	Set partition policy	-	Partition Policy Number, Value	-	None	HSM Security Officer (SO) - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
Query Audit Log Status	Display general status information of the audit log.	-	Session, log configuration parameter and value	Audit log status	None	Unauthenticated
Query HSM Configuration	Display configuration information	-	HSM Policy Number	HSM Policy Status	None	Unauthenticated
Query HSM Self-Test Status	Display self-test information	-	Command	Self-Test configuration, time period, last result, last failed test result	None	Unauthenticated
Query Partition Configuration	Display partition configuration information.	-	Partition Policy	Partition Policy Status	None	Unauthenticated
Query Partition Status	Display general information for a partition.	-	Status information type	Partition label, serial number, state (user initialized, login required), number of objects, and storage space	None	Unauthenticated
Request HSM Self-Test	This service allows the self-test to be triggered on demand. The service supports the CAST and RNG test	-	Self-Test mask	-	None	Unauthenticated
Reseed DRBG	Reseed the DRBG with entropy	Implicit	Session, additional input string	-	Generate Entropy	HSM Security Officer (SO) - DRBG Seed : G,E - DRBG_C: E - DRBG_V: E - Entropy: G,E Crypto Officer (CO) - DRBG Seed : G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG_C: E - DRBG_V: E - Entropy: G,E
Show Status	Display general status information	-	Command	Module status (zeroized, initialized), authenticated roles for active session, number of configured partitions, general error messages, and logs.	None	Unauthenticated
Show Version	Display versioning information	-	Command	Hardware, bootloader and firmware versions, and module serial number	None	Unauthenticated
Sign	Generate a signature over a block of user supplied data.	Implicit	Session, algorithm, algorithm parameter, data to sign	Signature	Generate Random Data RSA Signature Generation ECDSA Signature Generation LMS Signature Generation ML-DSA PureSigGen ML-DSA PreHashSigGen	HSM Security Officer (SO) - MTK: E - SMK: E - Partition ECDSA Private Key: E - Partition LMS Private Key: E - Partition RSA Private Key: E - DRBG output: E - Partition ML-DSA Private Key: E Crypto Officer (CO) - MTK: E - USK: E - Partition ECDSA Private Key: E - Partition LMS Private Key: E - Partition RSA Private Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG output: E - Partition ML-DSA Private Key: E Crypto User (CU) - MTK: E - USK: E - Partition ECDSA Private Key: E - Partition LMS Private Key: E - Partition RSA Private Key: E - DRBG output: E - Partition ML-DSA Private Key: E
Symmetric Encrypt/Decrypt	Encrypt or decrypt a block of user-supplied data	Implicit	Session, algorithm, algorithm parameters, key handle, data to en/decrypt	En/decrypted data	Symmetric Encryption/Decryption Authenticated Symmetric Encryption/Decryption	HSM Security Officer (SO) - MTK: E - SMK: E - Partition Symmetric Key: E Crypto Officer (CO) - MTK: E - USK: E - Partition Symmetric Key: E Crypto User (CU) - MTK: E - USK: E - Partition Symmetric Key: E
User Partition Create	Creates a user account and partition, and the SSPs required to use both.	Implicit	Session, partition label, CO Auth data (Pwd Auth), Domain	CO Auth data (PED Auth)	Generate Random Data KTS-HMAC KTS-RSA	HSM Security Officer (SO) - PED Key Authentication Data: R,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- User Password: W,E - GSK: E - KCV: G,W,E - PEC: R - PEK: E - PSK: G - RDEK: E - RMAC: E - RPV: E - SGSK: E - USK: G,E - DRBG output: E - Challenge Secret: G,R
User Partition Delete	Deletes user partition and zeroizes all objects associated with the partition	-	Session	-	None	HSM Security Officer (SO) - Challenge Secret: Z - GSK: Z - KCV: Z - SGSK: Z - USK: Z - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-KEM Private Key: Z
Verify	Verify a signature over a block of user supplied data.	Implicit	Session, algorithm, algorithm parameter, data to verify, signature	Ruling	RSA Signature Verification ECDSA Signature Verification DSA Signature Verification LMS Signature Verification Symmetric Encryption/Decryption ML-DSA PureSigVer ML-DSA PreHasSigVer	HSM Security Officer (SO) - SMK: E - Partition DSA Public Key: E - Partition ECDSA Public Key: E - Partition LMS Public Key: E - Partition RSA Public Key: E - Partition ML-DSA Public Key: E Crypto Officer (CO) - USK: E - Partition DSA Public Key: E - Partition ECDSA Public Key: E - Partition LMS Public Key: E - Partition RSA Public Key: E - Partition ML-DSA Public Key: E Crypto User (CU) - USK: E - Partition DSA Public Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition ECDSA Public Key: E - Partition LMS Public Key: E - Partition RSA Public Key: E - Partition ML-DSA Public Key: E
Zeroize (HSM Factory Reset)	Deletes all roles, all users and objects and sets all HSM settings and policy to values defined in pre-loaded configuration files.	-	Command	Status	None	Unauthenticated - KCV: Z - SMK: Z - TVK: Z - USK: Z - Partition Symmetric Key: Z - Partition DSA Public Key: Z - Partition ECDSA Public Key: Z - Partition ECDSA Private Key: Z - Partition LMS Public Key: Z - Partition LMS Private Key: Z - Partition RSA Public Key: Z - Partition RSA Private Key: Z - Partition ML-DSA Public Key: Z - Partition ML-DSA Private Key: Z - Partition ML-KEM Public Key: Z - Partition ML-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						KEM Private Key: Z

Table 13: Approved Services

4.3.1 HSM Set Policy service

HSM policy can only be configured if the corresponding configuration item is enabled which is defined based on loaded configuration update files. If a given policy being set is a ‘destructive policy’ – changing the setting will trigger zeroization of all User data objects and User partition.

4.3.2 Partition Set Policy service

Partition policy can only be configured if dependencies at the HSM level of configurations and policy are met. If a given policy being set is a destructive policy – changing the setting will trigger zeroization of all User data objects stored in the User partition. This service is not possible for the Backup configuration.

4.3.3 Configuration update service

The configuration update file defines the default settings for one or a number of HSM or Partition level configuration and policy settings. Configuration update files are signed using RSA PKCS #1-v1.5 signature using SHA2-384 and 4096-bit modulus.

4.3.4 Audit Config service

This service is used to specify:

- which events are to be recorded in the audit log, and
- the location of the logging daemon used to extract log sections from the module.

4.4 Non-Approved Services

The module does not support a non-approved mode and does not offer any non-approved services.

4.5 External Firmware Loaded

The Luna T7 contains two firmware components: the Firmware and the Bootloader. The module only supports the loading of new Firmware components.

The Firmware component is digitally signed using a Thales TCT Manufacturing signature key using RSA (4096 bits) PKCS #1 V1.5 with SHA2-384. Once a firmware update is invoked, the module checks the authenticity of the new firmware. A successful verification will trigger an automatic reset of the module resulting in the zeroisation of all users and user objects.

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 140-3 validation.

5 Firmware Security

5.1 Integrity Techniques

The Bootloader performs a SHA-1 integrity check of itself and a SHA2-256 integrity check of the Firmware it loads on each power-on and reset cycle. The module will halt if either integrity check fails.

5.2 Initiate on Demand

Using lunacm (provided with the LUNA client)

The default install location of lunacm on a Linux host is "/usr/safenet/lunaclient/bin" and on a Windows host is "C:\Program Files\SafeNet\LunaClient".

To initiate the integrity test

Using the slot command, ensure that the appropriate Luna T7 is selected. First, list the installed Luna Cryptographic Modules. Enter the following at the "lunacm:>" prompt:

- slot list

If more than one module is installed, select the appropriate Luna T7. Enter the following at the "lunacm:>" prompt replacing <slot> with the actual slot number:

- slot set –s <slot>

Initiate the integrity test. Enter the following at the "lunacm:>" prompt:

- hsm reset

This command runs other tests (i.e. algorithm self-tests) in addition to the integrity test. The command will return a result of "No Error" only if all of the tests pass.

Using lunash (requires SSH on the host)

Using SSH, log into the appliance as the appliance administrator. From a command prompt, enter the following, replacing <ip> with the ip address of Luna Network HSM (T-Series):

- ssh admin@<ip>

To initiate the integrity test

Enter the following at the lunash:> prompt:

- sysconf appliance reboot

Confirm the operation by entering "proceed" at the prompt.

This will reboot the Luna Network HSM (T-Series) resetting the installed Luna T7. During the reboot the SSH connection will be closed.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The Luna T7 has been validated to security level 3. This section is not applicable.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-evident enclosure	On receipt of module following transport. At any point following any un-authorized access to the environment hosting the module. Following any extended periods of unattended storage for the module After the module has been dropped or physically or environmentally stressed.	The outer cover of the module is embedded in the epoxy that encapsulates everything within the cryptographic boundary. Examine the aluminum shell for bends and look for broken or missing pieces of epoxy.

Table 14: Mechanisms and Actions Required

The Luna T7 is a multi-chip embedded module as defined by FIPS 140-3 standard ISO/IEC 19790:2012 section 7.7.1. The module is encased in a rigid metal enclosure that is bound to the module's circuitry by potting epoxy. Any tampering that might compromise a module's security is detectable by visual inspection of the module. The HSM Security Officer (SO) should perform a visual inspection of the module at regular intervals. Attempts to remove the enclosure will cause sufficient damage to the cryptographic module so that it is rendered inoperable.

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
HighTemperature	95 C	EFP	External Tamper Event: NVRAM Memory is wiped, processor exception occurs and the module halts operation and must be reset.
HighVoltage	13.5V	EFP	Processor exception occurs and the module halts operation and must be reset.
LowTemperature	-10 C	EFP	External Tamper Event: NVRAM Memory is wiped, processor exception occurs and the module halts operation and must be reset.
LowVoltage	10.5V	EFP	Processor exception occurs and the module halts operation and must be reset.

Table 15: EFP/EFT Information

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/under voltage, the module will reset itself and clear all working memory.

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

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
HighTemperature	+95.9 C
LowTemperature	-10 C

Table 16: Hardness Testing Temperatures

As disclosed above, the rigidity (hardness) of the module enclosure has been tested at the actual operational temperature range rather than the intended operational temperature range.

7.7 Additional Information

7.7.1 Secure Transport Mode

When configured to use PED-Authentication, the Luna T7 supports placing the device in Secure Transport Mode (STM). Placing the module in STM zeroizes the Master Tamper Key (MTK). The MTK wraps Partition Asymmetric Private Keys and Partition Symmetric Keys stored in the module. These keys are unavailable when in STM. The MTK, when created, is also stored as 2 splits. One split is internally stored. The other split (SRV) is stored on the Secure Recovery (Purple) PED Key. To exit STM the 2 splits, one internally supplied and the other supplied by the owner of the Secure Recovery PED Key, are used to reconstitute the MTK. Once reconstituted, the wrapped Partition Asymmetric Private Keys and Partition Symmetric Keys are available for use.

To enter secure transport mode in LunaSH, run the command "hsm srk transportmode enter". If the module is installed in a PCIe slot of a customer's workstation, to enter STM, use LunaCM. Using LunaCM, run the command "srk transport".

Refer to user documentation for more information on STM.

7.7.2 Temperature ranges

The Luna T7 has been designed to operate between 0 and 50°C, and to be stored between -20 and 60°C.

8 Non-Invasive Security

The Luna T7 does not implement any non-invasive mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Firmware	Firmware image	Static
Flash	256MB Flash	Static
NVRAM	Battery backed NVRAM	Static
RAM	2GB DDR3L RAM	Dynamic

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
ICD_I	PCIe	RAM	Plaintext	Manual	Electronic	
ICD_O	RAM	PCIe	Plaintext	Manual	Electronic	
MFR_I	-	Firmware	Plaintext	Manual	Electronic	
PIN_I	PCIe	RAM	Encrypted	Manual	Electronic	KTS-RSA
RPED_I	PCIe	RAM	Encrypted	Automated	Electronic	KTS-HMAC
RPED_O	RAM	PCIe	Encrypted	Automated	Electronic	KTS-HMAC
TPED_I	PED Serial	RAM	Plaintext	Manual	Electronic	
TPED_O	RAM	PED Serial	Plaintext	Manual	Electronic	
WICD_I	PCIe	RAM	Encrypted	Manual	Electronic	KTS-AES
WICD_O	RAM	PCIe	Encrypted	Manual	Electronic	KTS-AES

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Auto	Zeroize following use	RAM memory used to store an SSP is zeroized when SSP is no longer needed. SSPs are replaced with zeros.	N/A
CO	Deletes CO/CU keys used for authentication, user partition(s), and partition keys.	From the perspective of a CO user, resets the HSM back to its state first initialized by the SO. SO and Audit Officer are not zeroized. SSPs are replaced with zeros.	Changing setting of a destructive policy will delete all user partitions. Three Ten consecutive failed CO login attempts will delete that user's partition if not set to allow SO to re-enable user
Decom	Decommission the module by zeroizing KEK, TVK, and MTK	Zeroizing KEK and MTK disables access to all partition asymmetric and symmetric keys. Zeroizing KEK and TVK disables login for all users. The KEK, TVK, and MTK are replaced with zeros.	Short the two pins of the Decommission port
HSM	Deletes all keys used for authentication (SO, Audit, CO/CU), all user partitions, partition keys, and TVK.	Resets the HSM back to its state when received from the factory. SSPs are replaced with zeros.	ICD Command
Reboot	Zeroizes all RAM	SSPs stored in RAM prior to the reboot are zeroized. SSPs are replaced with random data.	Reboot the module
SO	Deletes SO and CO/CU keys used for authentication, all user	Resets the HSM back to its state when received from the factory except that the Audit Officer is	Three consecutive failed SO login attempts

Zeroization Method	Description	Rationale	Operator Initiation
	partitions, partition keys, and TVK.	maintained. SSPs are replaced with zeros.	
Tamper	Zeroizes the MTK.	All partition keys are encrypted by the MTK and become unusable when the MTK has been zeroized. The MTK itself is replaced with zeros.	Enter secure transport mode or short the two pins of the Tamper port

Table 19: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CITS-DAC	Device Authentication Certificate. Used for a specific PKI implementation requiring assurance that a key or a specific action originated within the HSM	4096 - 150	Asymmetric - PSP	RSA Key Pair Generation		
CITS-DAK	Device Authentication Key. Used for a specific PKI implementation requiring assurance that a key or a specific action originated within the HSM.	4096 - 150	Asymmetric - CSP	RSA Key Pair Generation		RSA Signature Generation
CKEV	Cloning Key Encryption Vector. Protects partition cryptographic objects during cloning	256 - 256	Symmetric - CSP		KAS-RSA	KTS-AES
Challenge Response	A value used for authentication in the challenge response scheme. It is generated using the challenge secret and the one-time random challenge value.	256 - 75	Authentication - CSP	Login with PED key		
Challenge Secret	Used with MFA. A random string generated by the cryptographic module, masked to printable characters, and output via the PED display when the user is created.	128 - 75	Authentication - CSP	Generate Random Data		
DRBG Seed	Seed material obtained from the entropy source. For seeding: entropy input, nonce and personalization string. For reseeding: entropy input and additional input.	512 or 640 - 443 to 560	DRBG Seed - CSP	Generate Random Data		Generate Random Data
DRBG output	Random numbers used in cryptographic algorithms	256 - 256	DRBG - CSP	Generate Random Data		
DRBG_C	DRBG internal state value	440 - 440	DRBG State - CSP	Generate Random Data		Generate Random Data
DRBG_V	DRBG internal state value	440 - 440	DRBG State - CSP	Generate Random Data		Generate Random Data
EC Peer public key	Imported public key used in KAS-ECC to establish a secure tunnel with a remote PED	P-384 - 192	Asymmetric - PSP			KAS-ECC
EC Private key	Local private key used in KAS-ECC to establish a secure tunnel with a remote PED	P-384 - 192	Asymmetric - CSP	ECDSA Key Generation		KAS-ECC
EC Public key	Local public key used in KAS-ECC to establish a secure tunnel with a remote PED	P-384 - 192	Asymmetric - PSP	ECDSA Key Generation		KAS-ECC
EC Shared secret	Shared secret established by KAS-ECC	192 - 192	Shared secret - CSP		KAS-ECC	Two-Step KDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Entropy	Entropy buffer populated from entropy source and consumed by DRBG	2048 - 1773 or 1792	Entropy - CSP	Generate Entropy		Generate Random Data
FSC	Firmware Signing Certificate. Used to verify Firmware images on initial load.	4096 - 150	Asymmetric - PSP			RSA Signature Verification
GSK	Global Storage Key. Protects static module parameters.	256 - 256	Symmetric - CSP			Symmetric Encryption/Decryption
HOC	Hardware Origin Certificate.	4096 - 150	Asymmetric - PSP	RSA Key Pair Generation		
HOK	Hardware Origin Key. Used to sign certificates for other device messaging key pairs.	4096 - 150	Asymmetric - CSP	RSA Key Pair Generation		RSA Signature Generation
KCV	Key Cloning Vector. Used to restrict a module's ability to participate in the cloning protocol as part of the OtherInfo for the KAS used to establish CKEV and SADK. 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.	384 - 384	Secret - CSP	Generate Random Data		KAS-RSA
KEK	Key Encryption Key. Encrypts login sensitive values.	384 - 256	Symmetric - CSP	Symmetric Key Generation		Symmetric Encryption/Decryption
LSC	License Signing Certificate. Used to verify Configuration Update images on initial load.	4096 - 150	Asymmetric - PSP			RSA Signature Verification
MIC	Manufacturer's Integrity Certificate. Used in verifying Hardware Origin Certificates (HOCs).	4096 - 150	Asymmetric - PSP			RSA Signature Verification
MTK	Master Tamper Key. Protects partition asymmetric private keys and symmetric keys stored in Flash.	256 - 256	Symmetric - CSP			Symmetric Encryption/Decryption
PEC	Password Encryption Certificate. Used for secure transport of password data.	4096 - 150	Asymmetric - PSP	RSA Key Pair Generation		KTS-RSA
PED Key Authentication Data	Used with PED Key and MFA authentication. A random value that is generated by the module when a SO, AO or CO is created. It is written to the role user's PED Key. It is input from the role user's PED Key as part of Login command.	384 - 384	Authentication - CSP	Generate Random Data		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PEK	Password Encryption Key. Protects user passwords provided to the module.	4096 - 150	Asymmetric - CSP	RSA Key Pair Generation		KTS-RSA
PSK	PIN Storage Key. Encrypts the SMK and partition USKs.	384 - 256	Symmetric - CSP	KTS-RSA		Symmetric Encryption/Decryption
Partition DSA Public Key	Public Key for a User partition	2048-3072 - 112-128	Asymmetric - PSP		KTS-AES	DSA Signature Verification
Partition ECDSA Private Key	Private Key for a User partition	P-224/P-384/P-521 - 112-256	Asymmetric - CSP	ECDSA Key Generation	KTS-AES	ECDSA Signature Generation
Partition ECDSA Public Key	Public Key for a User partition	P-224/P-384/P-521 - 112-256	Asymmetric - PSP	ECDSA Key Generation	KTS-AES	ECDSA Signature Generation ECDSA Signature Verification
Partition LMS Private Key	Private Key for a User partition	416 to 512 - 192/256	Asymmetric - CSP	LMS Key Pair Generation		LMS Signature Generation
Partition LMS Public Key	Public Key for a User partition	384/448 - 192/256	Asymmetric - PSP	LMS Key Pair Generation	KTS-AES	LMS Signature Generation LMS Signature Verification
Partition ML-DSA Private Key	Private Key for a User partition	2560/4032/4896 bytes - 128/192/256	Asymmetric - CSP	ML-DSA Key Generation		ML-DSA PureSigGen
Partition ML-DSA Public Key	Public Key for a User partition	1312/1952/2592 bytes - 128/192/256	Asymmetric - PSP	ML-DSA Key Generation		ML-DSA PureSigVer
Partition ML-KEM Private Key	Private Key used for key derivation and decapsulation	1632/2400/3168 bytes - 128/192/256	Asymmetric - CSP	KEM KeyGen KEM Encaps KEM Decaps		KEM Decaps
Partition ML-KEM Public Key	Public Key used for key derivation and encapsulation	800/1184/1568 bytes - 128/192/256	Asymmetric - PSP	KEM KeyGen		KEM Encaps KEM Decaps
Partition RSA Private Key	Private Key for a User partition	2048-4096 - 112-150	Asymmetric - CSP	RSA Key Pair Generation	KTS-AES	RSA Signature Generation
Partition RSA Public Key	Public Key for a User partition	2048-4096 - 112-150	Asymmetric - PSP	RSA Key Pair Generation	KTS-AES	RSA Signature Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						RSA Signature Verification
Partition Symmetric Key	Symmetric Key for a User partition	128-256 - 128-256	Symmetric - CSP	Symmetric Key Generation KEM Encaps	KTS-AES KEM Decaps	Symmetric Encryption/Decryption Authenticated Symmetric Encryption/Decryption Hash Message Authentication Cryptographic Message Authentication KTS-AES Key-Based KDF
RDEK	Remote (PED session) Data Encryption Key. Protects RPED tunnel across command interface to Remote PED.	384 - 256	Symmetric - CSP		KAS-ECC	Symmetric Encryption/Decryption
RMAC	Remote (PED session) Message Authentication Code Key. Authenticates RPED tunnel across command interface to Remote PED.	256 - 256	Authentication - CSP		KAS-ECC	Hash Message Authentication
ROOT	Root Certificate. Used in verifying other certificates.	4096 - 150	Asymmetric - PSP			RSA Signature Verification
RPV	Remote PED Vector. A randomly generated secret, shared with a Remote PED to establish a secure communication channel.	256 - 256	Generic Secret - CSP	Generate Random Data		KAS-ECC
RSA Shared secret	Shared secret established by KAS2 key agreement	4096/6144/8192 - 112/128/150	Shared secret - CSP		KAS-RSA	Two-Step KDF
Random Challenge	Used with PED Key and MFA authentication. A one-time random number generated by the cryptographic module and sent to the calling application for each login. It is XORed with the input Challenge Secret to compute the one-time response that is returned to the cryptographic module	192 - 192	Nonce - PSP	Generate Random Data		
SADK	Secure Audit Domain Key. Derived for a cloning domain based upon KCV that is used to wrap/unwrap the SALK when it is exported / imported from / to the module.	256 - 256	Symmetric - CSP	Two-Step KDF		KTS-AES
SALK	Secure Audit Logging Key. Authenticates log messages.	256 - 256	Authentication - CSP	Symmetric Key Generation	KTS-AES	Hash Message Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SGSK	Secondary Global Storage Key. Protects ephemeral module parameters.	256 - 256	Symmetric - CSP	Symmetric Key Generation		Symmetric Encryption/Decryption
SMK	Security (Officer) Master Key. Protects private objects owned by the SO.	256 - 256	Symmetric - CSP			Symmetric Encryption/Decryption
SRV	Secure Recovery Vector. 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.	256 - 256	Symmetric - CSP	Symmetric Key Generation		
TUK	Token (or Module) Unwrapping Key. Used in the cloning protocol.	4096 - 150	Asymmetric - CSP	RSA Key Pair Generation		KAS-RSA
TVK	Token (or Module) Variable Key. Protects cached User authentication data when auto-activation is enabled.	256 - 256	Symmetric - CSP			Symmetric Encryption/Decryption
TWC	Token (or Module) Wrapping Certificate. Used as part of the cloning protocol	4096 - 150	Asymmetric - PSP	RSA Key Pair Generation		KAS-RSA
U2K	U2 Key. Generic secret key loaded at manufacturing and used as shared secret to derive product specific keys	192 - 192	Generic Secret - CSP			Two-Step KDF
USK	User Storage Key. Protects private objects owned by the User.	256 - 256	Symmetric - CSP	Symmetric Key Generation		Symmetric Encryption/Decryption
User Password	User provided 8-255 character string.	64-2040 - -	Password - CSP			KTS-RSA

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CITS-DAC	ICD_O	RAM:Plaintext		Reboot	CITS-DAK:Paired With HOK:Signed by
CITS-DAK		Flash:Encrypted RAM:Plaintext		Reboot	CITS-DAC:Paired With
CKEV		RAM:Plaintext		Auto	KCV:Derived From RSA Shared secret:Derived From
Challenge Response	TPED_I RPED_I	RAM:Plaintext		Auto	Challenge Secret:Derived From Random Challenge:Derived From
Challenge Secret	TPED_O RPED_O	Flash:Encrypted		HSM SO CO	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Seed		RAM:Plaintext		Reboot	Entropy:Extracted from
DRBG output		RAM:Plaintext		Reboot	DRBG_C:Derived From DRBG_V:Derived From
DRBG_C		RAM:Plaintext		Reboot	DRBG Seed :Derived From
DRBG_V		RAM:Plaintext		Reboot	DRBG Seed :Derived From
EC Peer public key	ICD_I	RAM:Plaintext		Auto	
EC Private key		RAM:Plaintext		Auto	EC Public key:Paired With
EC Public key	ICD_O	RAM:Plaintext		Auto	EC Public key:Paired With
EC Shared secret		RAM:Plaintext		Auto	EC Private key:Established from EC Peer public key:Established from
Entropy		RAM:Plaintext		Reboot	
FSC	ICD_I	RAM:Plaintext		Reboot	ROOT:Signed by
GSK	MFR_I	Flash:Encrypted RAM:Plaintext		Reboot HSM SO CO	TUK:Encrypts HOK:Encrypts U2K:Encrypts CITS-DAK:Encrypts
HOC	MFR_I ICD_O	Flash:Encrypted			
HOK		Flash:Encrypted RAM:Plaintext		Reboot	
KCV	TPED_I TPED_O RPED_O RPED_I	Flash:Encrypted		HSM SO	
KEK		NVRAM:Plaintext		Decom	SMK:Encrypts USK:Encrypts PEK:Encrypts
LSC	ICD_I	RAM:Plaintext		Reboot	ROOT:Signed by
MIC	MFR_I ICD_O	Flash:Encrypted RAM:Plaintext		Reboot	ROOT:Signed by
MTK	MFR_I	NVRAM:Plaintext		Tamper Decom	Partition Symmetric Key:Encrypts Partition DSA Public Key:Encrypts Partition ECDSA Public Key:Encrypts Partition ECDSA Private Key:Encrypts Partition LMS Public Key:Encrypts Partition LMS Private Key:Encrypts Partition RSA Public Key:Encrypts Partition RSA Private Key:Encrypts
PEC	ICD_O	RAM:Plaintext		Reboot	User Password:Encrypts PEK:Paired With HOK:Signed by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
PED Key Authentication Data	TPED_I TPED_O RPED_O RPED_I	RAM:Plaintext Flash:Encrypted		Reboot HSM SO	
PEK		RAM:Plaintext		Reboot	User Password:Decrypts PEC:Paired With
PSK		RAM:Plaintext		Reboot Auto	User Password:Derived From USK:Encrypts SMK:Encrypts
Partition DSA Public Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
Partition ECDSA Private Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
Partition ECDSA Public Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
Partition LMS Private Key		Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
Partition LMS Public Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
Partition ML-DSA Private Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	Partition ML-DSA Public Key:Paired With
Partition ML-DSA Public Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	Partition ML-DSA Private Key:Paired With
Partition ML-KEM Private Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	Partition ML-KEM Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Partition ML-KEM Public Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	Partition ML-KEM Private Key:Paired With
Partition RSA Private Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
Partition RSA Public Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
Partition Symmetric Key	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted		Reboot HSM SO CO	
RDEK		RAM:Plaintext		Reboot Auto	Challenge Secret:Encrypts PED Key Authentication Data:Encrypts RPV:Derived From EC Shared secret:Derived From
RMAC		RAM:Plaintext		Reboot Auto	RPV:Derived From EC Shared secret:Derived From
ROOT	MFR_I ICD_O	Flash:Encrypted RAM:Plaintext		Reboot	
RPV	TPED_O	Flash:Encrypted RAM:Plaintext		Reboot	
RSA Shared secret		RAM:Plaintext		Auto	TUK:Established from TWC:Established from
Random Challenge	ICD_O	RAM:Plaintext		Auto	
SADK		Flash:Plaintext		Reboot	U2K:Derived From KCV:Derived From SALK:Encrypts
SALK	WICD_I WICD_O	Flash:Plaintext		Reboot HSM SO CO	
SGSK		Flash:Encrypted RAM:Plaintext		Reboot HSM SO CO	Challenge Secret:Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SMK		Flash:Encrypted RAM:Plaintext		Reboot HSM SO	
SRV	TPED_I TPED_O RPED_O RPED_I	Flash:Encrypted RAM:Plaintext		Reboot	MTK:Derived From
TUK		Flash:Encrypted RAM:Plaintext		Reboot	TWC:Paired With
TVK		NVRAM:Plaintext		Decom HSM SO CO	PED Key Authentication Data:Encrypts
TWC	ICD_O	RAM:Plaintext		Reboot	TUK:Paired With HOK:Signed by
U2K	MFR_I	Flash:Encrypted RAM:Plaintext		Reboot Auto	GSK:Encrypts SGSK:Encrypts KCV:Encrypts Partition Symmetric Key:Encrypts Partition DSA Public Key:Encrypts Partition ECDSA Public Key:Encrypts Partition ECDSA Private Key:Encrypts Partition LMS Public Key:Encrypts Partition LMS Private Key:Encrypts Partition RSA Public Key:Encrypts Partition RSA Private Key:Encrypts
USK		Flash:Encrypted RAM:Plaintext		Reboot HSM SO CO	GSK:Encrypts SGSK:Encrypts KCV:Encrypts Partition Symmetric Key:Encrypts Partition DSA Public Key:Encrypts Partition ECDSA Public Key:Encrypts Partition ECDSA Private Key:Encrypts Partition LMS Public Key:Encrypts Partition LMS Private Key:Encrypts Partition RSA Public Key:Encrypts Partition RSA Private Key:Encrypts
User Password	PIN_I	RAM:Encrypted		Reboot Auto	

Table 21: SSP Table 2

9.5 Transitions

The module implements the following security methods that are forecasted to transition to non-approved over the lifetime of the validation:

Algorithm	Uses
SHA-1	The module does not use SHA-1 directly to support a claim of security
SHA2-224	For hashing In RSA signature generation In ECDSA signature generation
SHA3-224	For hashing In RSA signature generation In ECDSA signature generation
HMAC-SHA-1	For MAC Generation As the PRF in PBKDF
HMAC-SHA2-224	For MAC Generation As the PRF in PBKDF As the PRF in KBKDF
HMAC-SHA3-224	For MAC Generation As the PRF in PBKDF As the PRF in KBKDF

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Bootloader integrity	SHA-1	EDC	SW/FW Integrity	Log message, Module halt on failure, Boot on success	Bootloader verifies its own image
Firmware integrity	SHA2-256	KAT	SW/FW Integrity	Log message, Module halt on failure, Boot on success	Bootloader verifies firmware image

Table 22: Pre-Operational Self-Tests

On power-on/reset, the integrity of the bootloader image and firmware image is verified. Once verified, the firmware tests the operation of the random number generator and the cryptographic algorithms.

10.2 Conditional Self-Tests

The module performs the following conditional self-tests. The module contains two implementations of some cryptographic algorithms. The module performs self-tests of both implementations.

In the table below,

- (FW) indicates that the self-test exercises the implementation of the algorithm in the Firmware cryptographic library.
- (HW) indicates that the self-test exercises the implementation of the algorithm in the Hybrid cryptographic library, which makes use of hardware cryptographic accelerators.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (FW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-CBC (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-CFB128 (FW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-CFB128 (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-CFB8 (FW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-CFB8 (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-CTR (FW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-CTR (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-ECB (FW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-ECB (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-GCM (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-KW (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-KWP (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-OFB (FW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
AES-OFB (HW)	128, 192 & 256-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS (HW)	256, 512-bit	KAT	CAST	Log message	Encrypt, Decrypt	On boot
APT	Adaptive proportion test	FDT	CAST	Function Fail / Error Logged / Module Halt	-	On generation
CMAC (FW)	128	KAT	CAST	Log message	Generate	On boot
CMAC (HW)	128	KAT	CAST	Log message	Generate	On boot
DRBG (HW)	SHA2-256	KAT	CAST	Log message	Instantiate, Generate, Reseed	On boot
DSA SigVer (FW)	L=1024, SHA 1; L=2048, SHA2-224	KAT	CAST	Log message	Verify	On boot
DSA SigVer (HW)	L=1024, SHA 1; L=2048, SHA2-224	KAT	CAST	Log message	Verify	On boot
ECDSA Key pairs	-	PCT	PCT	Function Fail	Sign and verify	On key pair generation
ECDSA SigGen	Curve: P-256 Hash: SHA2-256	KAT	CAST	Log message	Sign	On boot
ECDSA SigGen (HW)	Curve: P-256 Hash: SHA2-256	KAT	CAST	Log message	Sign	On boot
ECDSA SigVer (FW)	Curve: P-256 Hash: SHA2-256	KAT	CAST	Log message	Verify	On boot
ECDSA SigVer (HW)	Curve: P-256 Hash: SHA2-256	KAT	CAST	Log message	Verify	On boot
Firmware Load Test	RSA 4096-bit, SHA2-384	SigVer	SW/FW Load	Function Fail / Error Logged	Verify	On firmware load
GMAC (HW)	128-bits	KAT	CAST	Log message	Generate	On boot
HMAC-SHA-1 (FW)	256-bit key	KAT	CAST	Log message	Generate	On boot
HMAC-SHA-1 (HW)	256-bit key	KAT	CAST	Log message	Generate	On boot
HMAC-SHA-2 (FW)	256 & 1048 bit keys, SHA2-224, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Log message	Generate	On boot
HMAC-SHA-2 (HW)	256 & 1048 bit keys, SHA2-224, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Log message	Generate	On boot
HMAC-SHA-3 (FW)	256 & 1048 bit keys, SHA3-224, SHA3-256, SHA3-384, SHA3-512	KAT	CAST	Log message	Generate	On boot
HMAC-SHA-3 (HW)	256 & 1048 bit keys, SHA3-224, SHA3-256, SHA3-384, SHA3-512	KAT	CAST	Log message	Generate	On boot
KAS-ECC-SSC (FW)	P-192, P-224, P-256, P-384, P-521	KAT	CAST	Log message	Compute	On boot
KAS-ECC-SSC (HW)	P-192, P-224, P-256, P-384, P-521	KAT	CAST	Log message	Compute	On boot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-IFC-SSC (FW)	2048-bit modulo	KAT	CAST	Log message	Compute	On boot
KAS-IFC-SSC (HW)	2048-bit modulo	KAT	CAST	Log message	Compute	On boot
KBKDF (FW)	CMAC-AES	KAT	CAST	Log message	Derive	On boot
KBKDF (HW)	CMAC-AES	KAT	CAST	Log message	Derive	On boot
KDA TwoStep (FW)	CMAC-AES, Counter mode	KAT	CAST	Log message	Derive	On boot
KDA TwoStep (HW)	CMAC-AES, Counter mode	KAT	CAST	Log message	Derive	On boot
KTS-IFC (FW)	4096-bit, SHA2-512	KAT	CAST	Log message	Encrypt, decrypt	On boot
KTS-IFC (HW)	4096-bit, SHA2-512	KAT	CAST	Log message	Encrypt, decrypt	On boot
LMS Key pairs	-	PCT	PCT	Function Fail	Sign and verify	On key pair generation
LMS KeyGen (FW)	LMS_SHA256_M24_H5, LMS_SHA256_M32_H5	KAT	CAST	Log message	Generate	On boot
LMS KeyGen (HW)	LMS_SHA256_M24_H5, LMS_SHA256_M32_H5	KAT	CAST	Log message	Generate	On boot
LMS SigGen (FW)	LMS: SHA256_M24_H5 & SHA256_M32_H5, LMOTS: SHA256_N24_W2 & SHA256_N32_W1	KAT	CAST	Log message	Sign	On boot
LMS SigGen (HW)	LMS: SHA256_M24_H5 & SHA256_M32_H5, LMOTS: SHA256_N24_W2 & SHA256_N32_W1	KAT	CAST	Log message	Sign	On boot
LMS SigVer (FW)	All supported parameter sets	KAT	CAST	Log message	Verify	On boot
LMS SigVer (HW)	All supported parameter sets	KAT	CAST	Log message	Verify	On boot
ML-DSA Key pairs	-	PCT	PCT	Function Fail	Sign and Verify	On key pair generation
ML-DSA KeyGen (FW)	ML-DSA-44, ML-DSA-65, ML-DSA-87	KAT	CAST	Log message	Generate	On boot
ML-DSA KeyGen (HW)	ML-DSA-44, ML-DSA-65, ML-DSA-87	KAT	CAST	Log message	Generate	On boot
ML-DSA SigGen (FW)	ML-DSA-44, ML-DSA-65, ML-DSA-87, All Rejection outcomes`	KAT	CAST	Log message	Sign	On boot
ML-DSA SigGen (HW)	ML-DSA-44, ML-DSA-65, ML-DSA-87, All Rejection outcomes	KAT	CAST	Log message	Sign	On boot
ML-DSA SigVer (FW)	ML-DSA-44, ML-DSA-65, ML-DSA-87	KAT	CAST	Log message	Verify	On boot
ML-DSA SigVer (HW)	ML-DSA-44, ML-DSA-65, ML-DSA-87	KAT	CAST	Log message	Verify	On boot
ML-KEM Decap (FW)	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Log message	Decapsulate	On boot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ML-KEM Decap (HW)	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Log message	Decapsulate	On boot
ML-KEM Encap (FW)	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Log message	Encapsulate	On boot
ML-KEM Encap (HW)	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Log message	Encapsulate	On boot
ML-KEM Key pairs	-	PCT	PCT	Function Fail	Encapsulate and decapsulate	On key pair generation
ML-KEM KeyGen (FW)	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Log message	Generate	On boot
ML-KEM KeyGen (HW)	ML-KEM-512, ML-KEM-768, ML-KEM-1024	KAT	CAST	Log message	Generate	On boot
PBKDF (FW)	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Log message	Derive	On boot
PBKDF (HW)	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	KAT	CAST	Log message	Derive	On boot
RCT	Repetition count test	FDT	CAST	Function Fail / Error Logged / Module Halt	-	On generation
RSA SigGen (FW)	2048-bit, SHA2-256	KAT	CAST	Log message	Sign	On boot
RSA SigGen (HW)	2048-bit, SHA2-256	KAT	CAST	Log message	Sign	On boot
RSA SigVer (FW)	4096-bit, SHA2-256	KAT	CAST	Log message	Verify	On boot
RSA SigVer (HW)	4096-bit, SHA2-256	KAT	CAST	Log message	Verify	On boot
RSA key pairs	-	PCT	PCT	Function Fail	Sign and Verify	On key pair generation
SHA-1 (FW)	-	KAT	CAST	Log message	Hash	On boot
SHA-1 (HW)	-	KAT	CAST	Log message	Hash	On boot
SHA-2 (FW)	SHA2-224, SHA2-256, SHA2-348, SHA2-512	KAT	CAST	Log message	Hash	On boot
SHA-2 (HW)	SHA2-224, SHA2-256, SHA2-348, SHA2-512	KAT	CAST	Log message	Hash	On boot
SHA-3 (FW)	SHA3-224, SHA3-256, SHA3-348, SHA3-512	KAT	CAST	Log message	Hash	On boot
SHA-3 (HW)	SHA3-224, SHA3-256, SHA3-348, SHA3-512	KAT	CAST	Log message	Hash	On boot
TDES-CBC (FW)	-	KAT	CAST	Log message	Decrypt	On boot
TDES-CBC (HW)	-	KAT	CAST	Log message	Decrypt	On boot
XTS duplicate key	Verifying that the two keys are different	CT	Critical Function	Function Fail / Error Logged	-	On encrypt and decrypt operations

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Bootloader integrity	EDC	SW/FW Integrity	-	-
Firmware integrity	KAT	SW/FW Integrity	-	-

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (FW)	KAT	CAST	CAST Timer	Automatic
AES-CBC (HW)	KAT	CAST	CAST Timer	Automatic
AES-CFB128 (FW)	KAT	CAST	CAST Timer	Automatic
AES-CFB128 (HW)	KAT	CAST	CAST Timer	Automatic
AES-CFB8 (FW)	KAT	CAST	CAST Timer	Automatic
AES-CFB8 (HW)	KAT	CAST	CAST Timer	Automatic
AES-CTR (FW)	KAT	CAST	CAST Timer	Automatic
AES-CTR (HW)	KAT	CAST	CAST Timer	Automatic
AES-ECB (FW)	KAT	CAST	CAST Timer	Automatic
AES-ECB (HW)	KAT	CAST	CAST Timer	Automatic
AES-GCM (HW)	KAT	CAST	CAST Timer	Automatic
AES-KW (HW)	KAT	CAST	CAST Timer	Automatic
AES-KWP (HW)	KAT	CAST	CAST Timer	Automatic
AES-OFB (FW)	KAT	CAST	CAST Timer	Automatic
AES-OFB (HW)	KAT	CAST	CAST Timer	Automatic
AES-XTS (HW)	KAT	CAST	CAST Timer	Automatic
APT	FDT	CAST	-	-
CMAC (FW)	KAT	CAST	CAST Timer	Automatic
CMAC (HW)	KAT	CAST	CAST Timer	Automatic
DRBG (HW)	KAT	CAST	CAST Timer	Automatic
DSA SigVer (FW)	KAT	CAST	CAST Timer	Automatic
DSA SigVer (HW)	KAT	CAST	CAST Timer	Automatic
ECDSA Key pairs	PCT	PCT	-	-
ECDSA SigGen	KAT	CAST	CAST Timer	Automatic
ECDSA SigGen (HW)	KAT	CAST	CAST Timer	Automatic
ECDSA SigVer (FW)	KAT	CAST	CAST Timer	Automatic
ECDSA SigVer (HW)	KAT	CAST	CAST Timer	Automatic
Firmware Load Test	SigVer	SW/FW Load	-	-
GMAC (HW)	KAT	CAST	CAST Timer	Automatic
HMAC-SHA-1 (FW)	KAT	CAST	CAST Timer	Automatic
HMAC-SHA-1 (HW)	KAT	CAST	CAST Timer	Automatic
HMAC-SHA-2 (FW)	KAT	CAST	CAST Timer	Automatic
HMAC-SHA-2 (HW)	KAT	CAST	CAST Timer	Automatic
HMAC-SHA-3 (FW)	KAT	CAST	CAST Timer	Automatic
HMAC-SHA-3 (HW)	KAT	CAST	CAST Timer	Automatic
KAS-ECC-SSC (FW)	KAT	CAST	CAST Timer	Automatic
KAS-ECC-SSC (HW)	KAT	CAST	CAST Timer	Automatic
KAS-IFC-SSC (FW)	KAT	CAST	CAST Timer	Automatic
KAS-IFC-SSC (HW)	KAT	CAST	CAST Timer	Automatic
KBKDF (FW)	KAT	CAST	CAST Timer	Automatic
KBKDF (HW)	KAT	CAST	CAST Timer	Automatic
KDA TwoStep (FW)	KAT	CAST	CAST Timer	Automatic
KDA TwoStep (HW)	KAT	CAST	CAST Timer	Automatic
KTS-IFC (FW)	KAT	CAST	CAST Timer	Automatic
KTS-IFC (HW)	KAT	CAST	CAST Timer	Automatic
LMS Key pairs	PCT	PCT	-	-

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
LMS KeyGen (FW)	KAT	CAST	CAST Timer	Automatic
LMS KeyGen (HW)	KAT	CAST	CAST Timer	Automatic
LMS SigGen (FW)	KAT	CAST	CAST Timer	Automatic
LMS SigGen (HW)	KAT	CAST	CAST Timer	Automatic
LMS SigVer (FW)	KAT	CAST	CAST Timer	Automatic
LMS SigVer (HW)	KAT	CAST	CAST Timer	Automatic
ML-DSA Key pairs	PCT	PCT	-	-
ML-DSA KeyGen (FW)	KAT	CAST	CAST Timer	Automatic
ML-DSA KeyGen (HW)	KAT	CAST	CAST Timer	Automatic
ML-DSA SigGen (FW)	KAT	CAST	CAST Timer	Automatic
ML-DSA SigGen (HW)	KAT	CAST	CAST Timer	Automatic
ML-DSA SigVer (FW)	KAT	CAST	CAST Timer	Automatic
ML-DSA SigVer (HW)	KAT	CAST	CAST Timer	Automatic
ML-KEM Decap (FW)	KAT	CAST	CAST Timer	Automatic
ML-KEM Decap (HW)	KAT	CAST	CAST Timer	Automatic
ML-KEM Encap (FW)	KAT	CAST	CAST Timer	Automatic
ML-KEM Encap (HW)	KAT	CAST	CAST Timer	Automatic
ML-KEM Key pairs	PCT	PCT	-	-
ML-KEM KeyGen (FW)	KAT	CAST	CAST Timer	Automatic
ML-KEM KeyGen (HW)	KAT	CAST	CAST Timer	Automatic
PBKDF (FW)	KAT	CAST	CAST Timer	Automatic
PBKDF (HW)	KAT	CAST	CAST Timer	Automatic
RCT	FDT	CAST	-	-
RSA SigGen (FW)	KAT	CAST	CAST Timer	Automatic
RSA SigGen (HW)	KAT	CAST	CAST Timer	Automatic
RSA SigVer (FW)	KAT	CAST	CAST Timer	Automatic
RSA SigVer (HW)	KAT	CAST	CAST Timer	Automatic
RSA key pairs	PCT	PCT	-	-
SHA-1 (FW)	KAT	CAST	CAST Timer	Automatic
SHA-1 (HW)	KAT	CAST	CAST Timer	Automatic
SHA-2 (FW)	KAT	CAST	CAST Timer	Automatic
SHA-2 (HW)	KAT	CAST	CAST Timer	Automatic
SHA-3 (FW)	KAT	CAST	CAST Timer	Automatic
SHA-3 (HW)	KAT	CAST	CAST Timer	Automatic
TDES-CBC (FW)	KAT	CAST	CAST Timer	Automatic
TDES-CBC (HW)	KAT	CAST	CAST Timer	Automatic
XTS duplicate key	CT	Critical Function	-	-

Table 25: Conditional Periodic Information

The table above lists the self-tests performed on a periodic basis.

The timing of the periodic tests is controlled by a configurable parameter stored in Flash, with a minimum value of 1 hour and a default setting of 24 hours. When the timer expires, the ICD command interface is shut down and all command processing stops while the listed self-tests run on all cryptographic libraries.

The CAST test result is written to the driver log for the T7 module. On failure, the module will halt operation and stop processing commands until the next power cycle. On success, the module will re-enable its ICD command interface and resume normal operation.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Fatal Error	Error of severity that requires the module to halt operation	Failed integrity test Failed CAST	Power cycle	Red LED on device, Fatal Error status on display, Fatal Error message logged and sent to host, module operation halted
Service Error	Error on a function call that does not impact ability to operate securely	Failed PCT	Automatic	Error status returned in command response

Table 26: Error States

On the failure of a Pre-Operational Self Test or CAST, the module will log the failure, send the failure message to the host, and halt all operations. The only recovery from a Pre-Operational Self Test or CAST error is a power cycle.

10.5 Operator Initiation of Self-Tests

There are several ways in which an operator can initiate the Self-Test sequence on the module. One method is to simply perform a Power On reset sequence to run the POST tests.

The operator may also initiate the Request HSM Self-Test service by issuing the corresponding command across the ICD command interface.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Installation

Standard practice for high-value assets such as HSMs is installation in a secured environment. Installation in a secured environment is part of a defense-in-depth approach to minimize direct access to the HSM.

Securing the environment of the HSM typically will include a combination of both:

- securing its location using physical defenses; and
- procedures for monitoring and managing authorized access to the HSM.

The exact measures put in place will vary and should be commensurate with the potential consequences or costs associated with the complete compromise of the HSM and cryptographic keys (or data objects) it protects.

Common components of a physical security solution often include:

- dedicated areas (e.g. locked cage or cabinet) for the HSM as part of a general IT environment;
- monitored and audited physical access controls on IT environments hosting the HSM;
- hardened locks, doors and walls to increase the effort required to force access to the HSM;
- out-of-hours alarm systems on areas containing the HSM;
- 24hr/365day on-site or remote guard service that will respond to alarms; and
- video monitoring of areas containing the HSM to allow detection of activity in proximity to the HSM.

Refer to the Installation Guide in the Luna HSM documentation for steps to verify the integrity of the received product prior to installation and to install the product in your environment.

11.1.2 Initialization

Prior to use, the Luna T7 must be initialized per the instruction below. The operator assigned to the HSM's SO role may initialize the Luna T7 using the LunaCM application provided with the Luna client. The default install location of lunacm on a Linux host is "/usr/safenet/lunaclient/bin" and on a Windows host is "C:\Program Files\SafeNet\LunaClient".

Alternatively, the SO may initialize the Luna T7 using LunaSH. This requires SSH on the host device. Using SSH, log into the appliance as the appliance administrator. From a command prompt, enter the following:

```
ssh admin@<ip>
```

To initialize the module (via either LunaCM or LunaSH), invoke the "HSM Initialize" service by entering

```
hsm init -label <label> -password <password> -domain <domain> [ -
initwithped || -initwithpwd ]
```

`<label>` sets HSM's label. `<password>` sets the HSM's SO password. `<domain>` sets the HSM's domain (for use with cloning)

Next, configure the module to enforce FIPS requirements. If using LunaCM enter:

```
hsm changeHSMPolicy –policy 12 –value 0
```

If using LunaSH enter:

```
hsm changePolicy -policy 12 -value 0
```

Finally, verify that the FIPS policy has been set. If using LunaCM enter:

```
hsm showInfo
```

If using LunaSH enter:

```
hsm show
```

In the information provided by the command, look for:

```
*** The HSM is in FIPS 140-3 approved operation mode. ***
```

If the Luna T7 does not report the above, it has not been properly configured, and will be operating in a manner that is compliant with this security policy.

Refer to the Luna HSM documentation more information on LunaCM or LunaSH.

11.2 Administrator Guidance

Administrator guidance is provided in the following documents

- Configuration Guide
- Luna HSM Administration Guide

These documents, stored on digital media, are provided to customers with the product and are also available on the Customer Support Portal at https://support.thalestct.com.

11.2.1 PED Key management

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.

For specific guidance refer to the *PED Key Management* section of the *Luna HSM Administration Guide*. This guidance includes:

- Determining how many PED keys are needed
- Keeping a log of the operators in possession of PED keys
- Proper labelling of PED keys and HSM servers
- How to update PED keys
- Using M-of-N

11.3 Non-Administrator Guidance

In addition to the documentation provided for administrator guidance, other documentation, also provided with the product and available on the Customer Support Portal at https://support.thalestct.com include the following:

- Installation Guide
- LunaCM Command Reference Guide
- LunaSH Command Reference Guide
- SDK Reference Guide
- Utilities Reference Guide

11.6 End of Life

At the End of Life for the module, it is recommended that the HSM Factory Reset service be employed by use of the LunaCM ‘hsm factoryreset’ command. This will delete all HSM identities (including the SO), all users, keys, and data objects and sets all HSM settings and policies to factory default values.

It is further recommended that the Decommission input to the Luna T7 be asserted to zeroize nonvolatile memory.

12 Mitigation of Other Attacks

12.1 Attack List

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. The RSA blinding configuration option may be selected to mitigate this type of attack.