Thales Trusted Cyber Technologies

Luna M7 Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This non-proprietary document describes the security policy enforced by Thales Trusted Cyber Technologies' Luna M7 Cryptographic Module.

The Luna M7 Cryptographic Module can be used as follows:

- An embedded device in the Luna Backup HSM (T-Series)
  https://www.thalestct.com/hardware-security-modules/luna-backup-hsm/

- An embedded device in the Luna USB HSM (T-Series)
  https://www.thalestct.com/hardware-security-modules/tablet-hsm

This document applies to Luna M7 Cryptographic Module Hardware Version 872-500026-001 with Firmware Version 7.13.3 and Boot Loader Version 1.6.0.

The security policies described in this document apply to the Luna M7 Cryptographic Module only and do not include any security policy that may be enforced by the host appliance or server.

The policy of the Luna M7 Cryptographic Module can be configured for either Password or PED based authentication. The default setting is Password based authentication. The Security Officer (SO) can change the authentication mode between Password and PED. The configuration of the module can be verified by the operator by issuing a 'show policy' command that utilizes the Query HSM Configuration service.

At the time of manufacture, the Luna M7 Cryptographic Module is configured to be either a T-30B Luna Backup HSM (M7Backup) or a T-300 Luna USB HSM (M7Base). This status is indicated by the 'Enable full (non-backup) functionality' HSM capability bit (0=Backup HSM, 1=USB HSM) that is also shown as part of a 'show policy' command. A more limited set of Services is available to the Backup HSM; this is referred to as the Backup Configuration in this document.

Note: In the tables that follow, "N/A to Backup Config" in the Description field indicates this this is a service or other module feature that does not apply to the limited Backup Configuration in the M7Backup model.

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	N/A
	Overall Level	3

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Luna M7 Cryptographic Module is a multi-chip embedded hardware cryptographic module card that typically resides within a hand-held tablet device that connects to a computer workstation or server via USB. The Cryptographic Boundary of the module is contained in its own secure enclosure that provides physical resistance to tampering. The Cryptographic Boundary of the module is defined to encompass all components inside the secure enclosure.

Figure 1 shows a typical T-Series Luna USB HSM product that uses the Luna M7 Cryptographic Module. Figures 2 and 3 show the Cryptographic Boundary of the module.

The module may be explicitly configured to operate in either Approved mode, or in a Non-Approved mode of operation. Note that selection of operating in Approved mode occurs at initialization of the Cryptographic Module and cannot be changed during normal operation without zeroizing the module's non-volatile memory. Section 2.4 provides additional information for configuring the module in FIPS 140-3 Approved mode of operation.

The module only supports a single approved mode of operation. Any configuration changes to settings defining the 'Approved Mode of Operation' will trigger a zeroization of all CSPs and require the full reset and re-initialization of the module.

The module is accessed directly (i.e., electrically) over the USB communications interface. It also has a LCD screen interface that can be used to display system status. If configured, the Trusted Channel PIN Entry Device (PED), shown in Figure 4, can be connected to the module's USB Host port for authentication.

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

The module may host multiple user definitions or "user partitions" that are cryptographically separated and are presented as "virtual tokens" to user applications. A single "admin partition" exists that is dedicated to the HSM Security Officer role. Each partition must be separately authenticated in order to make it available for use.

A SmartCard interface is present at the cryptographic module physical perimeter but is unused in the certified configuration of the module.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

The Luna M7 Cryptographic Module is a multi-chip embedded hardware module which is typically used in a handheld tablet device such as the T-Series of the Luna Backup HSM and the Luna USB HSM. A T-Series Luna USB HSM and its external ports are shown in Figure 1.

Tested Operational Environment's Physical Perimeter (TOEPP):

The primary hardware component of the T-Series Luna USB HSM and Backup HSM is the 872-500026-001 Luna M7 Cryptographic Module. The cryptographically sensitive circuitry of the module is encased in an opaque, tamper-evident potting compound. The border of the potted region of the module defines the Cryptographic Boundary. Figure 2 shows the Top side of the 872-500026-001 Luna M7 Cryptographic Module and Figure 3 shows the Bottom side with the Cryptographic Boundary in red.

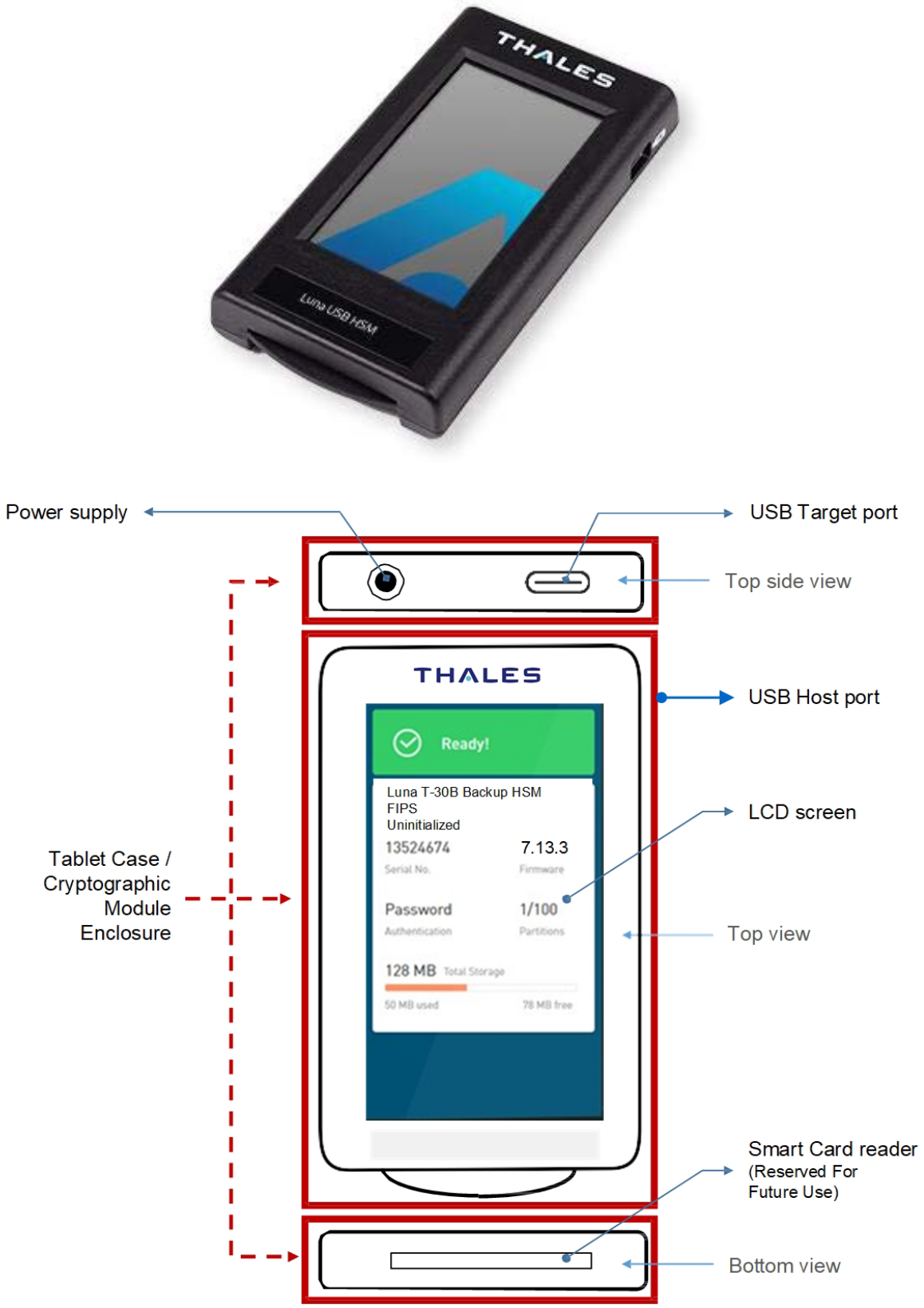

Figure 1: T-SERIES LUNA USB HSM Block Diagram, containing LUNA M7 Cryptographic Module, with external ports

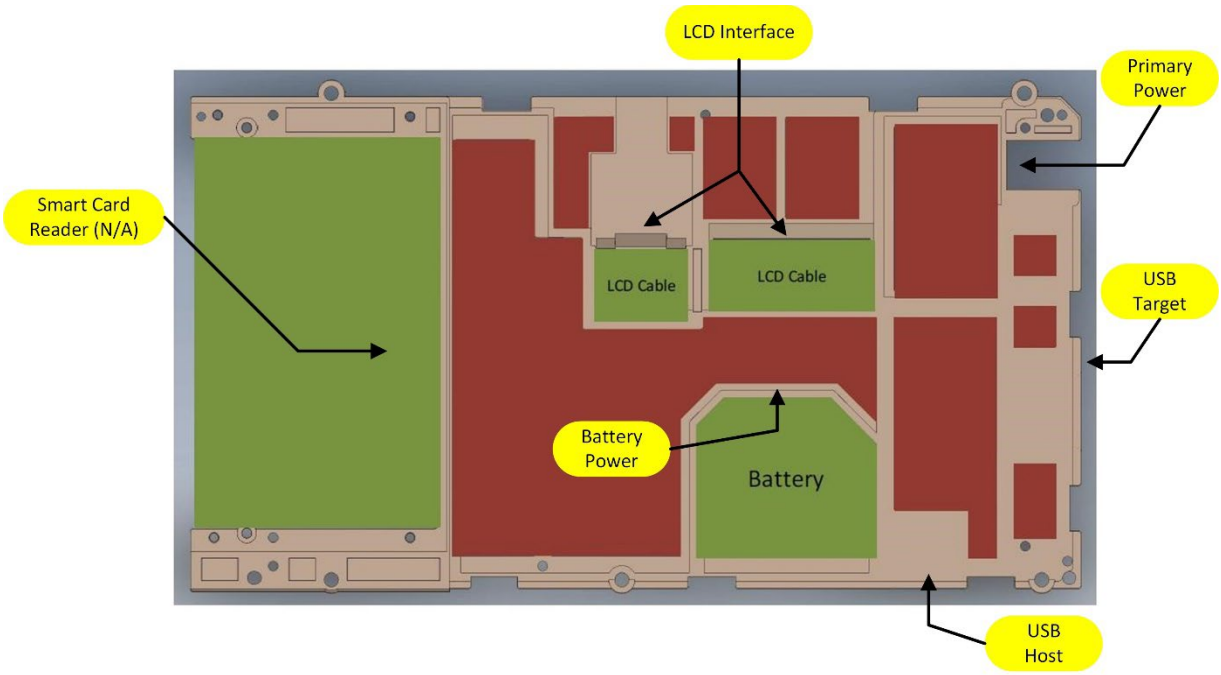

Figure 2: LUNA M7 Cryptographic Module, Front Side

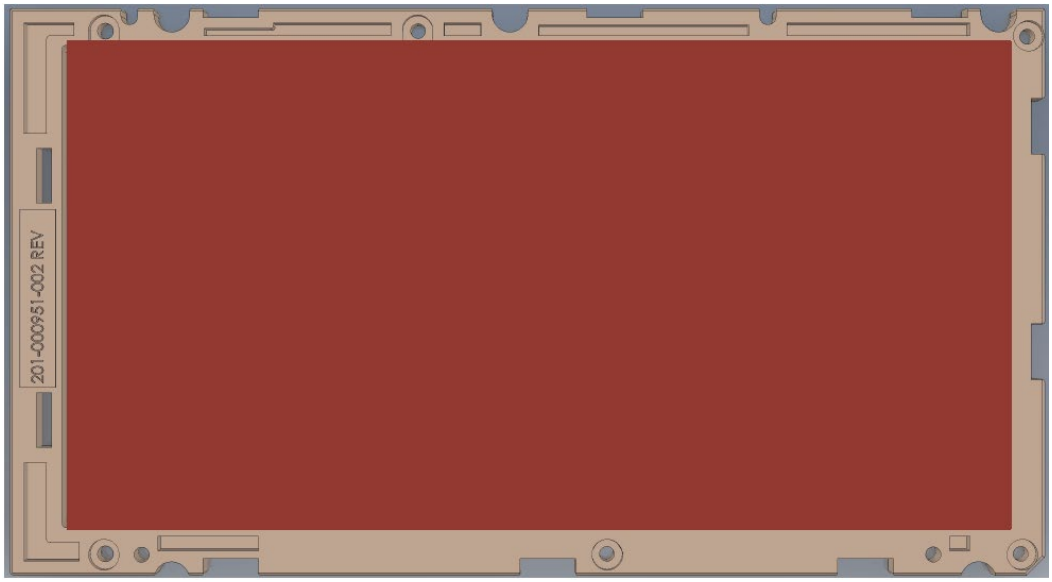

Figure 3: LUNA M7 Cryptographic Module, Rear Side

The regions in Red above represent the portion of the Cryptographic Boundary which is encapsulated in epoxy. The regions in Green are accessible physical ports such as the LCD Interface connectors, the Battery Power input, and the currently unused Smart Card Reader port.

The module includes a 3V coin cell battery, which is excluded from the FIPS 140-3 requirements. This battery is used to power the module's real-time clock on the Battery Power

interface when 5V is not supplied on the Primary Power interface. The real-time clock is not used to support any approved security functions supported by the module.
The smart card reader port and surrounding PCB board is also excluded from the FIPS 140-3 requirements since it is not used by the module.

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
M7Base or M7Backup	872-500026-001	7.13.3 with Bootloader Version: 1.6.0	NXP LS1021A with dual Arm Cortex-A7 cores	Base or Backup HSM in Approved mode, configured HSM services enabled

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

The following module components are not essential to the secure operation of the module and are excluded from the FIPS 140-3 requirements:

- 3V Coin Cell Battery (provides backup power to Real Time Clock)
- Smart Card Reader Port (unused in current module firmware)

The compromise of these components will not interfere with the approved operation of the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Base HSM Approved	M7Base model in Approved mode with all HSM services enabled	Approved	a) Status output on LCD Interface includes "FIPS" string and does not indicate "Backup HSM" b) lunacm 'hsm showinfo' reports 'The HSM is in FIPS 140-3 approved operation mode' and the Model is "M7Base".
Backup HSM Approved	M7Backup model in Approved mode with limited Backup HSM services enabled	Approved	a) Status output on LCD Interface includes "FIPS" string and indicates “Backup HSM”. b) lunacm 'hsm showinfo' reports “The HSM is in FIPS 140-3 approved operation mode” and the Model is “M7Backup”. c) lunacm ‘hsm showpolicies’ shows “Execute in non-FIPS

Mode Name	Description	Type	Status Indicator
			operation mode” is 0 and “Enable full (non-backup) functionality” is 0.
Base HSM Non-Approved	M7Base model in Non-Approved Mode with all HSM services enabled	Non-Approved	a) Status output on LCD Interface displays "Non-FIPS" string and does not indicate "Backup HSM" b) lunacm 'hsm showinfo' reports 'The HSM is *not* in FIPS 140-3 approved operation mode' and the Model is "M7Base". c) lunacm 'hsm showpolicies' shows "Execute in non-FIPs operation mode" is 1 and "Enable full (non-backup) functionality" is 1.
Backup HSM Non-Approved	M7Backup model in Non-Approved mode with limited Backup HSM services enabled	Non-Approved	a) Status output on LCD Interface displays "Non-FIPS" string and indicates “Backup HSM” b) lunacm 'hsm showinfo' reports “The HSM is *not* in FIPS 140-3 approved operation mode” and the Model is “M7Backup”. c) lunacm ‘hsm showpolicies’ shows “Execute in non-FIPS operation mode” is 1 and “Enable full (non-backup) functionality” is 0.

Table 3: Modes List and Description

Ahead of putting the module into its approved mode of operation, it is important to identify the hardware, firmware and bootloader versions of the target module and to check that these correspond to those listed in Section 1. The paragraphs below provide guidance on checking each element.

Any module returning hardware, firmware and bootloader versions not listed in Section 1 of this security policy is out of the scope of this validation and requires a separate FIPS 140-3 validation.

A number of T-Series HSM support applications, such as `lunacm` and its `slot list` and `slot info` commands, make calls to the Query HSM Status and Query HSM Configuration services to display the information necessary to verify the bootloader, firmware, and hardware versions and the Approved mode status.

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

```
[hsm] Boot Loader Revision M7 1.6.0.
```

The Luna M7 hardware model and firmware version can be displayed by the `lunacm` utility running on the module host. The `lunacm slot list` command provides an output similar to the following for a T-30B Backup HSM and a T-300 USB HSM, including the hardware model, backup configuration, and firmware version:

```
lunacm:>slot list
```

```
Slot Id ->              1
HSM Label ->            Luna T-30B Backup HSM Label
HSM Serial Number ->    700021
HSM Model ->            M7Backup
HSM Firmware Version -> 7.13.3
HSM Configuration ->    Luna UHD (PED) Backup Device
HSM Status ->           OK

Slot Id ->              2
HSM Label ->            Luna T-300 USB HSM Label
HSM Serial Number ->    700025
HSM Model ->            M7Base
HSM Firmware Version -> 7.13.3
HSM Configuration ->    Luna UHD (PED) Key Export With Cloning Mode
HSM Status ->           OK
```

To place the module in Approved mode as defined by FIPS PUB 140-3, the HSM Security Officer must disable the following module policy:

- "Execute in non-FIPS operation mode"

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

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

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

In compliance with IG:2.4.C, this module status as well as the Approved mode status conveyed on the LCD Interface (as indicated in Table 3) along with the service completion status shown in Table 13 provide an Indicator of when an Approved Service is used.

Mode Change Instructions and Status :

If the "Execute in non-FIPS operation mode" policy is "enabled", the Security Officer can use the `lunacm` tool to change that policy to "disabled" by use of the `hsm changeHSMpolicy` command to place the M7 module in the Approved Mode of Operation. This will result in a Firmware Zeroization (ZM4) that will erase all users, partitions, and cryptographic objects.

To complete the process of Zeroization for enabling Approved Mode, the user should also enter STM mode (ZM2) to erase the contents of nonvolatile RAM and then cycle power to the device to perform a power-up initialization (ZM1) as well.

If the need should arise to exit the Approved Mode of Operation, the process above is repeated, except that the "Execute in non-FIPS operation mode" policy is set to "enabled" to perform the

Firmware Zeroization (ZM4), which is then followed by the Secure Transport Mode (STM) mode (ZM2) and Power-On Reset (ZM1) zeroizations.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5021	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5021	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A5021	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A5021	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CMAC	A5022	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A5021	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5021	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A5022	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D
AES-GMAC	A5022	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KWP	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A5021	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-OFB	A5022	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A5022	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
DSA SigVer (FIPS186-4)	A5021	L - 1024, 2048, 3072 N - 160, 224, 256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
DSA SigVer (FIPS186-4)	A5022	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)	A5022	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5021	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5022	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A5021	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	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A5022	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	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A5021	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A5022	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
Hash DRBG	A5022	Prediction Resistance - No, Yes Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA-1	A5021	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA-1	A5022	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5021	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-224	A5022	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5021	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5022	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5021	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5022	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5021	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5022	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5021	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5022	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5021	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5022	Key Length - Key Length: 192-640 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5021	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5022	Key Length - Key Length: 192-1216 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5021	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5022	Key Length - Key Length: 192-1152 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5021	Domain Parameter Generation Methods - P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A5022	Domain Parameter Generation Methods - P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-IFC-SSC	A5021	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-basic Scheme - KAS2 - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-IFC-SSC	A5022	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-basic Scheme - KAS2 - KAS Role - initiator, responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KDA TwoStep SP800-56Cr2	A5021	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
KDA TwoStep SP800-56Cr2	A5022	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	A5021	KDF Mode - Counter Supported Lengths - Supported Lengths: 128-512 Increment 64	SP 800-108 Rev. 1
KDF SP800-108	A5022	KDF Mode - Counter Supported Lengths - Supported Lengths: 128-512 Increment 64	SP 800-108 Rev. 1
KTS-IFC	A5021	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
KTS-IFC	A5022	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	A5021	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 KeyGen	A5022	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	A5021	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	A5022	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	A5021	LMS Modes - LMS_SHA256_M24_H10, LMS_SHA256_M24_H15, LMS_SHA256_M24_H20,	SP 800-208

Algorithm	CAVP Cert	Properties	Reference
		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	
LMS SigVer	A5022	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
PBKDF	A5021	Iteration Count - Iteration Count: 10-1000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
PBKDF	A5022	Iteration Count - Iteration Count: 10-1000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-5)	A5022	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)	A5021	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigGen (FIPS186-5)	A5022	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A5021	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A5022	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A5021	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A5022	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1	A5021	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA-1	A5022	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-224	A5021	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-224	A5022	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	A5021	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	A5022	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	A5021	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A5022	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4
SHA2-512	A5021	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4
SHA2-512	A5022	Message Length - Message Length: 0-65336 Increment 8	FIPS 180-4
SHA3-224	A5021	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-224	A5022	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-256	A5021	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-256	A5022	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-384	A5021	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-384	A5022	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-512	A5021	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
SHA3-512	A5022	Message Length - Message Length: 0-65528 Increment 8	FIPS 202
TDES-CBC	A5021	Direction - Decrypt	SP 800-67 Rev. 2
TDES-CBC	A5022	Direction - Decrypt	SP 800-67 Rev. 2

Table 4: Approved Algorithms

The Approved algorithms implemented in the Luna M7 Cryptographic Module can be found in the table above. The algorithms listed for CAVP Cert #A5021 have been implemented in the Firmware cryptographic library in the module, which executes those algorithms using strictly firmware. The algorithms listed for CAVP Cert #A5022 have been implemented in the Hybrid cryptographic library, which uses a combination of firmware and hardware cryptographic accelerators to execute those algorithms.

The Hybrid cryptographic library is used to handle external cryptographic services requested by the user. When a CO invokes the Symmetric Encrypt service to encrypt a block of data using a key on the user's partition, the Hybrid library handles this operation to take advantage of the hardware acceleration for bulk encryption.

The Firmware cryptographic library is used to handle internal cryptographic operations – ones that are not invoked at the request of an external module user and do not involve user partition keys. As an example, when the module firmware updates a parameter in Flash that is encrypted by the Global Storage Key (GSK), the Firmware library handles that encryption operation.

One caveat to this framework is that all requests for random data generation, whether for internal or external operations, are passed to the Hybrid cryptographic library to use the approved SP 800-90A DRBG implemented in hardware.

Similar to Hash DRBG, these algorithms are only implemented with hardware acceleration and are only processed by the Hybrid cryptographic library (CAVP Cert. #A5022):

- AES-GCM
- AES-GMAC
- AES-KW
- AES-KWP
- AES-XTS

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG1	Key Type:Symmetric and Asymmetric	N/A	SP 800-133r2 Section 4 Scenario 1 - Used in methods 5.1, 5.2, 6.1 and 6.2
CKG2	Key Type:Symmetric	N/A	SP 800-133r2 6.3 Option 2 - Keys are generated per 6.3 with the key components being input into the module

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
DES	Symmetric Encryption/Decryption
Triple-DES	Symmetric Encryption
RC2	Symmetric Encryption/Decryption
RC4	Symmetric Encryption/Decryption
RC5	Symmetric Encryption/Decryption
CAST5	Symmetric Encryption/Decryption
MD2	Hash
MD5	Hash

Name	Use and Function
KECCAK	Hash
AES MAC (non-compliant)	Message Authentication Code
DES-MAC	Message Authentication Code
RC2-MAC	Message Authentication Code
RC5-MAC	Message Authentication Code
RIPEMD-160	Message Authentication Code
CAST3-MAC	Message Authentication Code
CAST5-MAC	Message Authentication Code
SSL3-MD5-MAC	Message Authentication Code
SSL3-SHA1-MAC	Message Authentication Code
HMAC (non-compliant less than 112 bits of encryption strength)	Message Authentication Code
DILITHIUM (PQC)	Asymmetric SigGen/SigVer, Generate Key
FALCON (PQC)	Asymmetric SigGen/SigVer, Generate Key
RSA X-509	Asymmetric SigGen/SigVer
RSA (non-compliant less than 112 bits of encryption strength)	Asymmetric SigGen/SigVer, Generate Key
DSA	Asymmetric SigGen, Generate Key
ECDSA (non-compliant less than 112 bits of encryption strength)	Asymmetric SigGen/SigVer, Generate Key
KYBER (PQC)	Generate Key, Key Agreement
SSL PRE-MASTER	Generate Key
Diffie-Hellman (key agreement; key establishment methodology; non-compliant less than 112 bits)	Key Agreement
RSA (key wrapping; key establishment methodology; non-compliant less than 112 bits of encryption strength)	Key Transport
RSA X9.31	Asymmetric SigGen
CAST3	Generate Key
RSA SigGen (sign using SHA-1 digest)	Asymmetric SigGen
ECDSA SigGen (sign using SHA-1 digest and B and K curves)	Asymmetric SigGen
ECDSA KeyGen (B and K curves)	Generate Key

Table 6: Non-Approved, Not Allowed Algorithms

Non-Approved security functions are not available for use when the module has been configured to operate in Approved Mode.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Generate Random Data	CKG DRBG ENT-ESV	Deterministic random bit generator		Hash DRBG: (A5022) CKG1: () Key Type:

Name	Type	Description	Properties	Algorithms
				Symmetric and Asymmetric
RSA Key Pair Generation	AsymKeyPair-KeyGen	Asymmetric key pair generation, RSA		RSA KeyGen (FIPS186-5): (A5022) CKG1: () Key Type: Symmetric and Asymmetric
RSA Signature Generation	DigSig-SigGen	Signature Generation, RSA		RSA SigGen (FIPS186-5): (A5022, A5021)
RSA Signature Verification	DigSig-SigVer	Signature Verification, RSA		RSA SigVer (FIPS186-5): (A5022, A5021)
ECDSA Key Generation	AsymKeyPair-KeyGen	Asymmetric key pair generation, ECDSA		ECDSA KeyGen (FIPS186-5): (A5022) Curves: Restricted to curves of P-224, P-256, P-384, P-521 CKG1: () Key Type: Symmetric and Asymmetric
ECDSA Signature Generation	DigSig-SigGen	Signature Generation, ECDSA		ECDSA SigGen (FIPS186-5): (A5022) Curves: Restricted to curves of P-224, P-256, P-384, P-521 ECDSA SigGen (FIPS186-5): (A5021)
ECDSA Signature Verification	DigSig-SigVer	Signature Verification, ECDSA		ECDSA SigVer (FIPS186-5): (A5022) Curves: Restricted to curves of P-224, P-256, P-384, P-521 ECDSA SigVer (FIPS186-5): (A5021)

Name	Type	Description	Properties	Algorithms
DSA Signature Verification (Legacy)	DigSig-SigVer	Signature Verification, DSA		DSA SigVer (FIPS186-4): (A5022, A5021)
LMS Key Pair Generation	AsymKeyPair-KeyGen	Asymmetric key pair generation, LMS		LMS KeyGen: (A5022, A5021) CKG1: () Key Type: Symmetric and Asymmetric
LMS Signature Generation	DigSig-SigGen	Signature Generation, LMS		LMS SigGen: (A5022, A5021)
LMS Signature Verification	DigSig-SigVer	Signature Verification, LMS		LMS SigVer: (A5022, A5021)
AES Symmetric Encryption/ Decryption	BC-UnAuth	Block Cipher, Unauthenticated, AES		AES-CBC: (A5022, A5021) AES-CFB128: (A5022, A5021) AES-CFB8: (A5022, A5021) AES-CTR: (A5022, A5021) AES-ECB: (A5022, A5021) AES-OFB: (A5022, A5021) AES-XTS Testing Revision 2.0: (A5022)
AES Authenticated Symmetric Encryption/ Decryption	BC-Auth	Block Cipher, Authenticated, AES		AES-GCM: (A5022)
TDES Symmetric Decryption (Legacy)	BC-UnAuth	Block Cipher, Unauthenticated, TDES Decryption		TDES-CBC: (A5022, A5021)
Secure Hash	SHA	Secure Hash		SHA-1: (A5022, A5021) SHA2-224: (A5022, A5021) SHA2-256: (A5022, A5021) SHA2-384: (A5022, A5021) SHA2-512: (A5022, A5021) SHA3-224: (A5022, A5021)

Name	Type	Description	Properties	Algorithms
				SHA3-256: (A5022, A5021) SHA3-384: (A5022, A5021) SHA3-512: (A5022, A5021)
Hash Message Authentication	MAC	Message Authentication, Secure Hash		HMAC-SHA2-224: (A5022, A5021) HMAC-SHA2-256: (A5022, A5021) HMAC-SHA2-384: (A5022, A5021) HMAC-SHA2-512: (A5022, A5021) HMAC-SHA3-224: (A5022, A5021) HMAC-SHA3-256: (A5022, A5021) HMAC-SHA3-384: (A5022, A5021) HMAC-SHA3-512: (A5022, A5021) HMAC-SHA-1: (A5022, A5021)
Cryptographic Message Authentication	MAC	Message Authentication, Symmetric Encryption		AES-CMAC: (A5022, A5021) AES-GMAC: (A5022)
KAS-ECC	KAS-Full	Shared Secret Calculation, KAS-ECC-SSC, followed by KAS Key Derivation Algorithm, KAS-56CKDF	IG: IG D.F Scenario 2 path (2), split Key Confirmation:No Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides 128	KAS-ECC-SSC Sp800-56Ar3: (A5022) Scheme: ephemeralUnified Domain Parameter Generation Methods: Curve P-384 KDA TwoStep SP800-56Cr2 KDF: Extraction-

Name	Type	Description	Properties	Algorithms
			bits of security strength	then-Expansion, Mac Modes: CMAC-AES-128 for Randomness Extraction and Key Expansion KAS-ECC-SSC Sp800-56Ar3: (A5021) Scheme: ephemeralUnified Domain Parameter Generation Methods: Curve P-384 KDA TwoStep SP800-56Cr2 KDF: CMAC-AES-128 for Randomness Extraction and Key Expansion
KAS-IFC	KAS-Full	Shared Secret Calculation, KAS IFC SSC, followed by KAS Key Derivation Algorithm, KAS-56CKDF	IG:IG D.F Scenario 1 path (2), split Key Confirmation:No Key Derivation:KDA (separately tested) Caveat:Key establishment methodology provides128 bits of security strength	KAS-IFC-SSC: (A5022, A5021) Scheme: KAS2 Key Generation Methods: rsakpg2-basic Hash Function Z: SHA2-512 KDA TwoStep SP800-56Cr2 KDF: Extraction-then-Expansion MAC Modes: CMAC-AES128 for both Randomness Extraction and Key Expansion
KTS-RSA	KTS-Unwrap KTS-Wrap	Wraps / Unwraps key data, RSA	Standard:SP 800-56Brev2 IG D.G:Approved per SP 800-56Brev2 using RSA 4096 Key confirmation:No	KTS-IFC: (A5022) Scheme: KTS-OAEP-Basic RSA-OAEP: Per SP800-56Br2 Mask Generation Function: SHA2-512

Name	Type	Description	Properties	Algorithms
			Caveat:Key establishment methodology provides 150 bits of security strength	KTS-IFC: (A5021) Scheme: KTS-OAEP-Basic RSA-OAEP: Per SP800-56Br2 Mask Generation Function: SHA2-512
KTS-AES	KTS-Unwrap KTS-Wrap	Wraps / Unwraps key data, AES Authenticated	Standard:SP 800-38F IG D.G:Approved Caveat:Key establishment provides between 128 and 256 bits of security strength	AES-GCM: (A5022) AES-KW: (A5022) AES-KWP: (A5022)
KAS Key Derivation Algorithm	KAS-56CKDF	SP800-56C Key Derivation, CMAC-AES128		KDA TwoStep SP800-56Cr2: (A5022) KDF: Extraction-then-Expansion MAC Modes: CMAC-AES128 for both Randomness Extraction and Key Expansion KDA TwoStep SP800-56Cr2: (A5021) KDF: Extraction-then-Expansion MAC Modes: CMAC-AES-128 for both Randomness Extraction and Key Expansion
Key-Based KDF	KBKDF	AES Key Based Key Derivation Function		KDF SP800-108: (A5022, A5021) KDF Mode: Counter MAC Mode: CMAC-AES128, CMAC-AES192, CMAC-AES256

Name	Type	Description	Properties	Algorithms
Password Based KDF	PBKDF	Password Based Key Derivation Function		PBKDF: (A5022) PBKDF2: using PKCS#5 HMAC Algorithm: HMAC-SHA-1 per SP800-132 Option 1a PBKDF: (A5021) PBKDF: using PKCS#5 HMAC Algorithm: HMAC-SHA-1 per SP800-132 Option 1a
Cryptographic Key Generation	CKG	Symmetric Key Generation from direct output of module DRBG. N/A to Backup Config		CKG1: () Key Type: Symmetric and Asymmetric
KTS-AES-HMAC	KTS-Unwrap KTS-Wrap	Wraps/Unwraps key data, HMAC Authenticated	Standard:SP 800-38F IG D.G:Approved Caveat:Key establishment provides 256 bits of security strength	AES-CBC: (A5022, A5021) SHA2-256: (A5022, A5021) HMAC-SHA2-256: (A5022, A5021)
RSA Signature Verification (Legacy)	DigSig-SigVer	Signature Verification, RSA		RSA SigVer (FIPS186-4): (A5022, A5021)
ECDSA Signature Verification (Legacy)	DigSig-SigVer	Signature Verification, ECDSA		ECDSA SigVer (FIPS186-4): (A5022) Curves: Restricted to curves of P-224, P-256, P-384, P-521 ECDSA SigVer (FIPS186-4): (A5021) Curves: Restricted to curves of P-224, P-256, P-384, P-521

Name	Type	Description	Properties	Algorithms
Split Key	CKG DRBG ENT-ESV	Generate Key splits from base symmetric key		Hash DRBG: (A5022) CKG2: ()
Recover Key	CKG	Recover base symmetric key from key splits		CKG2: ()

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

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) being generated inside the module's cryptographic boundary.

The IV generation supported in Approved mode is fixed 96-bit size that is generated with the SP800-90A Hash_DRBG (SHA2-256) output.

Since the IV is generated internally and is random and is fixed 96 bits in length, requirements from SP800-38D and IG:C.H are satisfied.

2) XTS-AES

The check for Key_1 ≠ Key_2 is done before using the keys in the XTS AES algorithm to process data and is in accordance with IG:C.I requirements. Key_1 and Key_2 are independently generated.

3) PBKDF

Password Length and Probability – In accordance with IG:D.N, refer to Section 4.1 below, Password Authentication Mode, 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 – The PBKDF is used internal to the cryptographic module to derive the storage encryption key used to encrypt the checkword used in Password Authentication Mode. The derived key is separately used to encrypt for storage the USK. The module uses method 1a from SP800-132 where the derived Master Key (MK) is used directly as the Data Protection Key (DPK).

4) SHA-1

SHA-1 is non-approved for digital signature generation and deprecated through December 31, 2030 for non-digital signature applications.

5) SHA3
In compliance with IG:C.C, all SHA3 supported functionality has been CAVP tested. This applies to the CAVP tests for SHA3-224, SHA3-256, SHA3-384, SHA3-512 as documented in Certificates #A5021 and #A5022. The module makes no Vendor Affirmed claims with regards to SHA3 and IG:C.C.

6) RSA
In compliance with IG:C.F, for RSA KeyGen, SigGen, and SigVer, the module only supports FIPS 186-5 moduli/key sizes 2048, 3072, and 4096 bits. The FIPS 186-4 key size of 1024 bits is supported for legacy SigVer. The CAVP testing of these algorithms and key sizes is captured in Certificates #A5021 and #A5022.

7) Legacy Algorithms
Triple-DES Decryption, DSA Signature Verification and RSA/ECDSA Signature Verification specific to FIPS 186-4 are legacy algorithms.
Algorithms designated as “Legacy” can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M

8) SP800-56Cr2 KDA TwoStep
Regarding IG:C.L D), the SP800-56Cr2 TwoStep KDA is implemented with CMAC-AES-128 for both the first step Randomness Extraction and the second step SP800-108 Key Expansion. The security strength of its derived key material is 128 bits. This also applies to the established keys for the following key agreement scheme Security Functions that use the SP800-56Cr2 KDA TwoStep algorithm:
ECC Key Agreement Scheme
RSA Key Agreement Scheme

2.8 RBG and Entropy

Cert Number	Vendor Name
E97	Thales

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Thales G7 Hardware Platform TRNG	Physical	NXP® QorIQ® LS1021A	1 bit	0.838411 bits	N/A

Table 9: Entropy Sources

1) Entropy Source

The Luna M7 Cryptographic Module incorporates Thales part 808-000080-001 featuring the NXP LS1021A SoC processor. The ESV certificate for the TRNG in this part is #E97 (https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/97).

On power-up hardware initialization, the Entropy Source is configured in accordance with the values specified in the Configuration Settings of the Public Use Document for the #E97 ESV certificate. The Entropy Source configuration settings are not modified after this initialization.

2) RBG

The ESV noise source is used exclusively to feed the hardware DRBG (Cert #A5022).

The noise source outputs blocks of entropy in 384 bits with H = 0.838411. Following testing, the DRBG is seeded with a 256-bit seed and a 128-bit nonce from the noise source containing 384 * 0.838411 which equals 321 bits of entropy.

Raw noise collection is performed autonomously by hardware as entropy is required to seed the on-chip DRBG. If the entropy register is not full when the DRBG accesses it, the read will stall until the entropy is generated. During each entropy collection cycle, 2500 samples of raw noise are collected.

All outputs from the noise source are subjected to statistical testing ahead of being fed to the DRBG. The output of the hardware noise source includes a total failure test to check for bit-patterns consistent with hardware failures.

3) RBG Output

The output of the DRBG is used for the Generate Random Data SFI and for Cryptographic Key Generation.

As noted in SP800-90Ar1, Section 8.6.7, the entropy input seed plus nonce loaded from the noise source to the Hash_DRBG (SHA2-256) must contain at least 3/2 security_strength bits of entropy. The 321 bits of entropy loaded from the noise source to the Hash_DRBG on instantiation gives a security_strength of 192 bits per SP800-90Ar1. When using the module's DRBG, the module generates SSPs (e.g. keys) and random strings whose strengths are modified by available entropy.

2.9 Key Generation

In accordance with FIPS 140-3 Implementation Guidance (IG) D.H requirements for Cryptographic Key Generation (CKG), symmetric cryptographic keys and seed for asymmetric key generation are generated by the direct unmodified output of the module's NIST SP800-90A DRBG, using Scenario 1 from Section 4 and Section 6.1 of SP800-133r2. Asymmetric Key pairs are generated based upon SP800-133r2 Sections 5.1 and 5.2.

The module supports derivation of Symmetric keys from other keys as per SP800-133r2, Section 6.2.2, and supports the derivation of Symmetric keys from passwords using methods in SP800-133r2, Section 6.2.3 and SP800-132 for storage encryption. Symmetric keys can also be

recovered from key components entered into the module using methods from SP800-133r2, Section 6.3, Option 2 (Exclusive-Oring of components); this is employed when the Master Tamper Key (MTK) is recovered from its key splits when exiting Secure Transport Mode (STM) as described in Section 7.5 below.

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

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

2.10 Key Establishment

2.10.1 Key Import and Export

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

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

The remaining keys and SSPs listed in Table 9.4 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:

2.10.2 Key Cloning

Key cloning uses a one-time derived AES key, the Cloning Key Encryption Vector (CKEV), as a session key to wrap (AES-KWP) an object being transferred from one cryptographic module to another. Objects transferred using the cloning protocol may be keys, user data, or module data. The AES session encrypting key (CKEV) is obtained first by using KAS-IFC-SSC (KAS2-basic) as the SP800-56Br2 compliant key agreement scheme between source and target modules, both of which share their Token Wrapping Certificates (TWCs), to provide the shared secret in compliance with IG:D.F Scenario 1 (2). Both parties use the agreed upon shared secret in a Two-Step Key Derivation Function with Randomness Extraction per SP800-56Cr2 and SP800-108 (KDA TwoStep SP800-56Cr2 and KDF SP800-108), with the distributed Key Cloning Vector (KCV) as part of the FixedInput, to derive matching session keys for the wrapping and unwrapping operations.

2.10.3 Key Wrap / Unwrap

The Wrap/Unwrap Key service, calling the AES Wrap/Unwrap Key security function (KTS-Wrap), encrypts an asymmetric or symmetric key value for output. In compliance with IG:D.G, this function either employs the SP800-38F algorithms AES-KW or AES-KWP or the authenticated symmetric encryption algorithm AES-GCM to perform symmetric key wrapping for transport.

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

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

2.10.4 Remote PED Tunnel

If configured, the user has the option of operating the Luna PED remotely, connected to a USB port on a management workstation. When using a Remote PED on a module in Approved Mode, an encrypted tunnel is established to wrap data exchanged across the module's command interface to the Remote PED device. The tunnel is based upon an AES-256-CBC data encryption key (RDEK) and an HMAC-SHA2-256 message authentication key (RMAC). The Remote PED tunnel invokes the AES HMAC Wrap/Unwrap Key security function (KTS-Wrap) to encrypt and authenticate the secure data exchanged using the RDEK and the RMAC, employing the combination method of key wrapping for transport in compliance with IG:D.G and SP 800-38F.

The RDEK and RMAC are established using an ECC Key Agreement Scheme (KAS-ECC-SSC). The module and the Remote PED participate in the Elliptic Curve Diffie-Hellman (ECC CDH, P-384) key agreement session as specified for the Ephemeral Unified Model in SP800-56Ar3. Both parties use the agreed upon shared secret in a Two-Step Key Derivation Function with Randomness Extraction per SP800-56Cr2 and SP800-108 (KDA TwoStep SP800-56Cr2 and KDF SP800-108) in compliance with IG:D.F Scenario 2 (2); the Remote PED Vector (RPV) is used as part of the FixedInput for the KDF. The KDF is used to derive the 384 bits of the RDEK (256-bit AES Key plus 128-bit IV) and the 256-bit RMAC to provide the key data for the Remote PED Tunnel.

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
USB Target	Data Input Data Output Control Input Status Output	Data I/O, Luna ICD, Remote PED Tunnel, Bootloader command protocol
USB Host	Data Input Data Output	Physical Trusted Channel (Local PED)
Smart Card reader port	Data Input Data Output	N/A - deactivated in certified firmware configuration and excluded from the FIPS 140-3 requirements

Physical Port	Logical Interface(s)	Data That Passes
LCD Interface	Status Output	System status
Power	Power	5V - generated from an external 12V power supply module or USB Target port 5V power, 3.6V (battery)

Table 10: Ports and Interfaces

The module supports the following physical ports and interfaces, as shown in Figure 2:

- USB Target port
- USB Host port
- LCD Interface port
- Smart Card reader port
- Power supply

3.2 Trusted Channel Specification

Physical Trusted Channel - Local PED

If configured, the Luna M7 Cryptographic Module can use a Luna PED (PIN Entry Device) as an external data input/output device. The Luna PED connects to the module's USB Host port and is used to pass authentication data and SSPs to and from the module via a physical trusted channel. SSPs that are output to the Luna PED are stored in a PED Key (also known as an iKey) USB device connected to the Luna PED.
Any PED Key, once data has been written to it, is an Identification and Authentication device and must be safeguarded accordingly by the administrative or operations staff responsible for the operation of the module within the customer's environment.

The figure below shows a Luna PED device and PED Keys. The Luna PED device connects to the Luna M7 Cryptographic Module Host USB port by USB cable.

Figure 4: LUNA PED AND PED Keys

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 (CO) 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 Vector/Key Cloning Vector (KCV), 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

IG 3.4.A declarations for the Local PED Trusted Channel

- To enable use of the Local PED Trusted Channel, the HSM Security Officer must enable the following module policy: “PED-based authentication”. The enabling of this policy

serves as an indication that PED Key Authentication is in use and the Local PED Trusted Channel is enabled.
The process by which the SO can set and view module policy using the `lunacm` tool and the `hsm changeHSMpolicy` command is described in Section 2.4 above.

- The USB Host port is distinct from other module ports and reserved for use as a Trusted Channel to the PED Device. All other USB devices on the USB Host port are disabled. The operator connects the PED Device to the module USB Host port with a USB cable to establish the Trusted Channel. The operator must remain in control of the module, the PED Device, and the connection USB cable when using the Trusted Channel.

- The service that transfers SSP data between the module and the PED Device on the Trusted Channel must be performed by an authenticated user. These services are initiated by a command received on a separate module interface – the USB Target (Luna ICD) port.

- The operator must insert the appropriate PED Key corresponding to the issued command and follow the prompted instructions initiated by the module and displayed on the PED Device for a successful transfer of data.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	User provided byte array (minimum 8 bytes). With a maximum of 3 failed consecutive login attempts per minute for the SO and 10 for other Users, the thresholds required by FIPS 140-3 can never be reached.	Memorized Secret	1 in 2^64	A maximum of 10 failed consecutive login attempts in one minute.
PED Key (if configured)	48-byte random authentication data generated when a role is initialized and stored on PED Key. With a maximum of 3 failed consecutive login attempts per minute for the SO and 10 for other Users, the threshold required by FIPS 140-3 can never be reached.	Multi Factor Crypto Device	1 in 2^384	A maximum of 10 failed consecutive login attempts in one minute.
PED Key plus Challenge Secret	48-byte random authentication data plus 16-byte Challenge Secret generated when a role is	Multi Factor Device plus	1 in 2^384	A maximum of 10 failed consecutive

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
password (if configured)	initialized and stored on PED Key. No additional security is claimed with the addition of the Challenge Secret. With a maximum of 3 failed consecutive login attempts per minute for the SO and 10 for other Users, the threshold required by FIPS 140-3 can never be reached.	Memorized Secret		login attempts in one minute.

Table 11: Authentication Methods

Roles, Services and Authentication adhere to FIPS 140-3 Security Level 3 requirements.

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 data supported for each role.

If configured with PED, all roles must authenticate using a PED Key. When a role is initialized under this configuration, a module generates the authentication data as a 48-byte random value and writes it to a PED Key. Two-Factor Authentication, with PED Key plus a Challenge Secret password, is mandatory for the Crypto User role. The additional Challenge Secret password authentication can optionally be assigned to the Crypto Officer role.

If configured with Password, all roles must authenticate using a password. When a role is initialized under this configuration, the operator enters the initial password for the role. In Approved mode, using KTS-IFC in compliance with SP800-56Br2, the password is delivered to the module encrypted with the module's Password Encryption Key (PEC) using RSA-OAEP and a random nonce to prevent replay attacks.

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.

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.

Activation

If PED is configured, the Crypto Officer and Crypto User roles can be configured to use a two-step authentication process. The first stage is termed "Activation" and is performed using a PED Key. Once activated, access to key material and cryptographic services is not allowed until the

second stage of authentication, “User Login”, has been performed using the role’s Challenge Secret password.

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

M of N

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

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

4.2 Roles

Name	Type	Operator Type	Authentication Methods
HSM Security Officer (SO)	Identity	Crypto Officer	Password PED Key (if configured)
Crypto Officer (CO)	Identity	User	Password PED Key (if configured) PED Key plus Challenge Secret password (if configured)
Crypto User (CU)	Identity	User	Password PED Key plus Challenge Secret password (if configured)
Audit Officer (AO)	Identity	Crypto Officer	Password PED Key (if configured)
Public User	Role	User	None

Table 12: Roles

The Luna M7 Cryptographic Module supports the following authenticated roles:

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

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

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

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

The module also supports the following unauthenticated role:

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

4.3 Approved Services

For the Indicator column in the Approved Services table, a ‘Successful Command Response’ indicates that:
The command return code is LUNA_RET_OK (0).
This along with the module policy “Execute in non FIPS operation mode” as identified in Section 2.4 is Disabled (0) indicate the module has executed an Approved service.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Query HSM Status	This service is used to retrieve general status information on the module including items such as: - hardware, bootloader and firmware versions; - module serial number; - module	Successful command response along with status as indicated in Table 3	Luna ICD command, status information type	Luna ICD response, HSM Status data	None	Public User Crypto Officer (CO) Crypto User (CU) HSM Security Officer (SO) Audit Officer (AO)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	state (e.g., zeroized, initialized); - authenticated roles for active session (if present); - number of configured partitions; and - general error messages and logs.					
HSM Factory Reset	Factory reset deletes all roles (including HSM SO), all users and objects and sets all HSM settings and policy to values defined in pre-loaded configuration update files.	Successful command response along with status as indicated in Table 3	Luna ICD command	Luna ICD response	None	Public User - SMK: Z - USK: Z - KCV: Z - TVK: Z - Partition Asymmetric Private Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z HSM Security Officer (SO) - SMK: Z - USK: Z - KCV: Z - TVK: Z - Partition Asymmetric Public Keys: Z - Partition Symmetric Keys: Z - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Asymmetric Private Keys: Z Crypto Officer (CO) - SMK: Z - USK: Z - KCV: Z - TVK: Z - Partition Asymmetric Public Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Private Keys: Z Crypto User (CU) - SMK: Z - USK: Z - KCV: Z - TVK: Z - Partition Asymmetric Public Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Private Keys: Z Audit Officer (AO) - SMK: Z - USK: Z - KCV: Z - TVK: Z - Partition Asymmetric Public Keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Symmetric Keys: Z - Partition Asymmetric Private Keys: Z
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; - 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	Successful command response along with status as indicated in Table 3	Luna ICD command, SO Authentication data (Pwd Auth), Cloning Domain, Label	Luna ICD response, SO Auth data (PED Auth)	Generate Random Data RSA Signature Verification AES Symmetric Encryption/ Decryption Hash Message Authentication KAS-ECC KTS-RSA Password Based KDF RSA Signature Verification (Legacy)	HSM Security Officer (SO) - DRBG_C: E - DRBG_V: E - PED Key Authentication Data: R,W,E - User Password: W,E - PEK: G,E - PEC: G,R - TUK: G - TWC: G - CITS-DAK: G - CITS-DAC: G - SMK: G,E - PSK: G,E - SGSK: G,E - KCV: G,W,E,Z - RDEK: G,E - RMAC: G,E - HOK: E - GSK: E - RPV: E - USK: Z - TVK: Z - Partition Asymmetric Private Keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z
User Partition Create	This service creates a user partition at the request of the HSM SO. The user partition is created in memory and the associated Crypto Officer role is created.	Successful command response along with status as indicated in Table 3	Luna ICD command, session partition label, CO Auth data (Pwd Auth), Domain	Luna ICD response, CO Auth data (PED Auth)	Generate Random Data AES Symmetric Encryption/ Decryption Hash Message Authentication KAS-ECC KTS-RSA Password Based KDF	HSM Security Officer (SO) - PED Key Authentication Data: R,W,E - User Password: W,E - USK: G,E - PSK: G - KCV: G,E - RDEK: G,E - RMAC: G,E - PEC: R - PEK: E - GSK: E - SGSK: E - RPV: E - DRBG_C: E - DRBG_V:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z
User Partition Delete	This service is used to delete an existing user partition. During deletion, the module zeroizes all objects associated with the partition	Successful command response along with status as indicated in Table 3	Luna ICD command, session	Luna ICD response	None	HSM Security Officer (SO) - USK: Z - GSK: Z - SGSK: Z - KCV: Z - Challenge Secret: Z - Partition Asymmetric Private Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z
Query Partition Status	This service is used to retrieve general status information on a target partition including items such	Successful command response along with status as indicate	Luna ICD command, status information type	Luna ICD response, partition status data	None	Public User HSM Security Officer (SO) Crypto Officer (CO) Crypto User (CU) Audit

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	as: - partition label and serial number; - partition state (user initialized, login required); - number of stored objects; and - used and free storage space.	d in Table 3				Officer (AO)
Crypto User Role Init	This service creates the limited Crypto User role on a partition at the request of the partition Crypto Officer	Successful command response along with status as indicated in Table 3	Luna ICD command, session	Luna ICD response, Challenge Secret	Generate Random Data AES Symmetric Encryption/ Decryption Hash Message Authentication KAS-ECC	Crypto Officer (CO) - Challenge Secret: G,R - RDEK: G,E - RMAC: G,E - SGSK: E - RPV: E - DRBG_C: E - DRBG_V: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Query HSM Configuration	This service is used to retrieve information on HSM configuration and policy settings.	Successful command response along with status as indicated in Table 3	Luna ICD command, HSM Policy Number	Luna ICD response, HSM Policy Status	None	Public User HSM Security Officer (SO) Crypto Officer (CO) Crypto User (CU) Audit Officer (AO)
Query Partition Configuration	This service is used to retrieve information on the configuration and policy settings for a target partition.	Successful command response along with status as indicated in Table 3	Luna ICD command, Partition Policy Number	Luna ICD response, Partition Policy Status	None	Public User HSM Security Officer (SO) Crypto Officer (CO) Crypto User (CU) Audit Officer (AO)
HSM Set Policy	This service is used to set available HSM policy settings. 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	Successful command response along with status as indicated in Table 3	Luna ICD command, session HSM Policy Number, Value	Luna ICD response	None	HSM Security Officer (SO) - USK: Z - GSK: Z - SGSK: Z - KCV: Z - Challenge Secret: Z - Partition Asymmetric Private Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	policy being set is a 'destructive policy' - changing the setting will trigger zeroization of all User data objects and User partition.					
Partition Set Policy	This service is used to set available partition policy settings. 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	Successful command response along with status as indicated in Table 3	Luna ICD command	Luna ICD response, session Partition Policy Number, Value	None	HSM Security Officer (SO) - Partition Asymmetric Private Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	partition. N/A to Backup Config					
Firmware Update	This service validates and then loads a new module firmware image (excluding bootloader). The replacement image is signed using RSA PKCS #1-v1.5 signature using SHA2-384 and 4096-bit modulus.	Successful command response along with status as indicated in Table 3	Luna ICD command	Luna ICD response, session, FUF (Signed Firmware Update File)	RSA Signature Verification TDES Symmetric Decryption (Legacy) RSA Signature Verification (Legacy)	HSM Security Officer (SO) - FSC: W - ROOT: E - GSK: E - U2K: E
Configuration Update	This service validates the signature on a loaded configuration update file ahead of its contents being stored on the module. The configuration update file defines the default	Successful command response along with status as indicated in Table 3	Luna ICD command	Luna ICD response, session, CUF (Signed Configuration Update File)	RSA Signature Verification RSA Signature Verification (Legacy)	HSM Security Officer (SO) - LSC: W - ROOT: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	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.					
Audit Role Init	This service creates the Audit Officer role on the HSM.	Successful command response along with status as indicated in Table 3	Luna ICD command, AO Auth Data (Pwd Auth), Domain	Luna ICD response, AO Auth Data (PED Auth)	Generate Random Data AES Symmetric Encryption/ Decryption Hash Message Authentication KAS-ECC KTS-RSA Password Based KDF	Public User - USK: G,E - PSK: G,E - KCV: G,E - RDEK: G,E - RMAC: G,E - PEC: R - PED Key Authentication Data: R,W,E - User Password: W,E - GSK: E - RPV: E - DRBG_C: E - DRBG_V: E - EC Private Key: G,E,Z - EC Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z HSM Security Officer (SO) - USK: G,E - PSK: G,E - KCV: G,E - RDEK: G,E - RMAC: G,E - PEC: R - PED Key Authentication Data: R - User Password: W,E - GSK: E - RPV: E - DRBG_C: E - DRBG_V: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Two-Step KDK: G,E,Z Crypto Officer (CO) - USK: G,E - PSK: G,E - KCV: G,E - RDEK: G,E - RMAC: G,E - PED Key Authentication Data: R - User Password: W,E - GSK: E - RPV: E - DRBG_C: E - DRBG_V: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z - PEC: R Crypto User (CU) - USK: G,E - PSK: G,E - KCV: G,E - RDEK: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PEC: R - PED Key Authentication Data: R - User Password: W,E - GSK: E - RPV: E - DRBG_C: E - DRBG_V: E - RMAC: G,E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z Audit Officer (AO) - USK: G,E - PSK: G,E - KCV: G,E - RDEK: G,E - RMAC: G,E - PEC: R - PED Key Authentication Data: R - User Password: W,E - GSK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- RPV: E - DRBG_C: E - DRBG_V: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z
Query Audit Log Status	This service is used to retrieve general status information on the secure audit log.	Successful command response along with status as indicated in Table 3	Luna ICD command	Luna ICD response, audit log status	None	Public User HSM Security Officer (SO) Crypto Officer (CO) Crypto User (CU) Audit Officer (AO)
Audit Config	This service is used to configure which audit events are to be recorded in the secure audit log and in addition to configure the location of the	Successful command response along with status as indicated in Table 3	Luna ICD command, session, log configuration parameter and value	Luna ICD response	Hash Message Authentication	Audit Officer (AO) - SALK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	secure logging daemon used to extract log sections from the module.					
Audit Log Secret Export/Import	This service exports or imports and encrypted copy of the SALK. This service can be used to allow validation of the authenticity of extracted log sections between modules	Successful command response along with status as indicated in Table 3	Luna ICD command, session, wrapped log secret (import)	Luna ICD response, wrapped log secret (export)	KTS-AES KAS Key Derivation Algorithm	Audit Officer (AO) - SADK: G,E - SALK: R,W - U2K: E - KCV: E - Two-Step KDK: G,E,Z
Audit Log Verify	This service checks both the integrity and authenticity of extracted sections of the secure module audit log.	Successful command response along with status as indicated in Table 3	Luna ICD command, session, audit log segment	Luna ICD response	Hash Message Authentication	HSM Security Officer (SO) - SALK: E Audit Officer (AO) - SALK: E
Enable STM	This service enables Secure Transport Mode functionalit	Successful command response along with	Luna ICD command, session	Luna ICD response, SRV	AES Symmetric Encryption/ Decryption KAS-ECC KTS-AES-HMAC	HSM Security Officer (SO) - RDEK: G,E - RMAC:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	y at the request of the SO. The SRV is erased from internal Flash and moved to the SO Purple PED key when STM is enabled.	status as indicated in Table 3			Recover Key	G,E - SRV: R,Z - RPV: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z
Enter STM	This service enters Secure Transport Mode at the request of the SO. When entering STM, the SRV is read from the SO Purple PED key and verified and the MTK is zeroized.	Successful command response along with status as indicated in Table 3	Luna ICD command, SRV	Luna ICD response	KAS-ECC KTS-AES	HSM Security Officer (SO) - MTK: G,Z - RDEK: G,E - RMAC: G,E - SRV: W,E - RPV: E - MTK_IS: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Request HSM Self-Test	This service allows the power-on self-test to be triggered on demand. The service supports re-run of the entire power-on self-test	Successful command response along with status as indicated in Table 3	Luna ICD command, Self-Test mask	Luna ICD response	Generate Random Data RSA Key Pair Generation RSA Signature Generation RSA Signature Verification ECDSA Key Generation ECDSA Signature Generation ECDSA Signature Verification DSA Signature Verification (Legacy) LMS Key Pair Generation LMS Signature Generation LMS Signature Verification AES Symmetric Encryption/ Decryption AES Authenticated Symmetric Encryption/ Decryption TDES Symmetric Decryption (Legacy) Secure	Public User - DRBG_C: E - DRBG_V: E HSM Security Officer (SO) - DRBG_C: E - DRBG_V: E Crypto Officer (CO) - DRBG_C: E - DRBG_V: E Crypto User (CU) - DRBG_C: E - DRBG_V: E Audit Officer (AO) - DRBG_C: E - DRBG_V: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Hash Hash Message Authentication Cryptographic Message Authentication KAS-ECC KAS-IFC KTS-RSA KTS-AES KAS Key Derivation Algorithm Key-Based KDF Password Based KDF RSA Signature Verification (Legacy) ECDSA Signature Verification (Legacy)	
Query HSM Self-Test Status	This service returns status information on the self-test results, including the self test time period, the time of the last self-test, the pass/fail result of the last self-test, the time of the last	Successful command response along with status as indicated in Table 3	Luna ICD command	Luna ICD response, Self-Test configuration, time period, last result, last failed test result	None	Public User HSM Security Officer (SO) Crypto Officer (CO) Crypto User (CU) Audit Officer (AO)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	failed test, and the result (function and failure code) of the last failed test.					
Partition Backup / Restore (Clone)	This service exports (Backup) or imports (Restore) data objects for a Crypto Officer partition as part of the Cloning protocol.	Successful command response along with status as indicated in Table 3	Luna ICD command, session, object handle (Backup), wrapped key object (Restore)	Luna ICD response, object handle (Restore), wrapped key object (Backup)	Generate Random Data RSA Signature Verification KAS-IFC KTS-AES RSA Signature Verification (Legacy)	HSM Security Officer (SO) - Partition Asymmetric Private Keys: R,W - Partition Symmetric Keys: R,W - ROOT: E - MIC: E - HOC: E - TWC: E - TUK: E - KCV: E - CKEV: G,E - MTK: E - USK: E - DRBG_C: E - DRBG_V: E - Partition Asymmetric Public Keys: R,W - RSA Peer Public Key: W,E - RSA Shared Secret: G,E,Z - Two-Step KDK: G,E,Z Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(CO) - Partition Asymmetric Private Keys: R,W - Partition Symmetric Keys: R,W - ROOT: E - MIC: E - HOC: E - TWC: E - TUK: E - KCV: E - CKEV: G,E - MTK: E - USK: E - DRBG_C: E - DRBG_V: E - Partition Asymmetric Public Keys: R,W - Two-Step KDK: G,E,Z - RSA Peer Public Key: W,E - RSA Shared Secret: G,E,Z
Login	This service is used to login as a given role (SO, CO, CU, AO) to a session setup between the client and a target	Successful command response along with status as indicated in Table 3	Luna ICD command,Role Auth Data, Challege Response (PED Key plus Challenge)	Luna ICD response, session, Random Challenge (PED Key plus Challenge)	Generate Random Data RSA Key Pair Generation RSA Signature Generation AES Symmetric Encryption/ Decryption	HSM Security Officer (SO) - PEK: G,E - PEC: G,R - TUK: G - TWC: G - CITS-DAK: G - CITS-DAC: G - PSK: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	partition. Following successful login, the authentication state for the associated session will be changed to that of the successfully authenticated role. Following login, the authentication state of the session is used check and track privileges associated with the role. If an SO Login fails and exceeds the threshold count, a Factory Reset zeroization occurs. If a CO Login fails and exceeds the threshold count, a User Partition Delete occurs.				Hash Message Authentication KAS-ECC KTS-RSA Password Based KDF KTS-AES-HMAC	- SGSK: G,E,Z - KCV: G,E,Z - RDEK: G,E - RMAC: G,E - PED Key Authentication Data: W,E - Challenge Response: W,Z - User Password: W,E - HOK: E - SMK: E,Z - USK: E,Z - GSK: E,Z - RPV: E - DRBG_C: E - DRBG_V: E - TVK: Z - Partition Asymmetric Private Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Shared Secret: G,E,Z - Two-Step KDK: G,E,Z Crypto Officer (CO) - Random Challenge: G,R,Z - PEK: G,E - PEC: G,E - TUK: G - TWC: G - CITS-DAK: G - CITS-DAC: G - PSK: G,E - SGSK: G,E,Z - KCV: G,E,Z - RDEK: G,E - RMAC: G,E - Challenge Response: W - PED Key Authentication Data: W,E - User Password: W,E - HOK: E - USK: E,Z - GSK: E,Z - RPV: E - DRBG_C: E - DRBG_V: E - Challenge Secret: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Partition Asymmetric Private Keys: Z - Partition Asymmetric Public Keys: Z - Partition Symmetric Keys: Z - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z Crypto User (CU) - Random Challenge: G,R - PEK: G,E - PEC: G,R - TUK: G - TWC: G - CITS-DAK: G - CITS-DAC: G - PSK: G,E - SGSK: G,E - KCV: G,E - RDEK: G,E - RMAC: G,E - Challenge

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Response: W - PED Key Authentication Data: W,E - HOK: E - USK: E - GSK: E - RPV: E - DRBG_C: E - DRBG_V: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z Audit Officer (AO) - PEK: G - PEC: G,R - TUK: G - TWC: G - CITS-DAK: G - CITS-DAC: G - PSK: G,E - KCV: G,E - RDEK: G,E - RMAC: G,E - PED Key Authenticat

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ion Data: W,E - User Password: W,E - HOK: E - USK: E - GSK: E - SGSK: G,E - RPV: E - DRBG_C: E - DRBG_V: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - Two-Step KDK: G,E,Z
Logout	This service logs an authenticated user out of the associated session for the given role.	Successful command response along with status as indicated in Table 3	Luna ICD command, session	Luna ICD response	None	Audit Officer (AO) Crypto User (CU) HSM Security Officer (SO) - Partition Asymmetric Private Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(CO) - Partition Asymmetric Private Keys: Z - Partition Symmetric Keys: Z - Partition Asymmetric Public Keys: Z
Initialize Remote PED Vector (RPV)	This service triggers creation of the module Remote PED Vector. As part of this service, the preshared secret RPV is stored locally in HSM Flash and written remotely to the RPV PED Key device.	Successful command response along with status as indicated in Table 3	Luna ICD command, session	Luna ICD response, RPV	Generate Random Data	HSM Security Officer (SO) - RPV: G,W - DRBG_C: E - DRBG_V: E
Generate Key	This service is used to generate symmetric keys or asymmetric key pairs requested by the end-user and stored in the corresponding cryptographic module	Successful command response along with status as indicated in Table 3	Luna ICD command, session, generation algorithm, algorithm parameter, key attributes	Luna ICD response, key handles	Generate Random Data RSA Key Pair Generation RSA Signature Generation RSA Signature Verification ECDSA Key Generation ECDSA Signature	HSM Security Officer (SO) - Partition Asymmetric Private Keys: G - Partition Symmetric Keys: G - SMK: E - MTK: E - DRBG_C: E - DRBG_V: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	partition for use or export. N/A to Backup Config.				Generation ECDSA Signature Verification LMS Key Pair Generation LMS Signature Generation LMS Signature Verification Cryptographic Key Generation RSA Signature Verification (Legacy) ECDSA Signature Verification (Legacy)	- Partition Asymmetric Public Keys: G Crypto Officer (CO) - Partition Asymmetric Private Keys: G - Partition Symmetric Keys: G - USK: E - MTK: E - DRBG_C: E - DRBG_V: E - Partition Asymmetric Public Keys: G
Derive Key	This service is used to derive keys based on other key material stored in the module partition or supplied to it on request of the end-user. Derived keys are stored in the module partition for use or export. N/A to Backup Config.	Successful command response along with status as indicated in Table 3	Luna ICD command, algorithm, algorithm parameters, derivation key handles	Luna ICD response, derived key handle	KAS-ECC KAS Key Derivation Algorithm Key-Based KDF	HSM Security Officer (SO) - Partition Symmetric Keys: G,E - Partition Asymmetric Public Keys: E - SMK: E - MTK: E - Partition Asymmetric Private Keys: Crypto Officer (CO) - Partition Symmetric Keys: G,E - Partition Asymmetri

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						c Private Keys: E - USK: E - MTK: E - Partition Asymmetric Public Keys: E
Wrap/Unwrap Key	This service is used to import or export user partition secret or private key objects using key wrapping as requested by the Crypto Officer. N/A to Backup Config.	Successful command response along with status as indicated in Table 3	Luna ICD command, wrapping key handle, key to wrap handle (Wrap), wrapped key blob (Unwrap), key attributes (Unwrap)	Luna ICD response, wrapped key blob (Wrap), unwrapped key handle (Unwrap)	KTS-AES	HSM Security Officer (SO) - Partition Asymmetric Private Keys: E - Partition Symmetric Keys: E - SMK: E - MTK: E Crypto Officer (CO) - Partition Asymmetric Private Keys: E - Partition Symmetric Keys: E - USK: E - MTK: E Crypto User (CU) - Partition Asymmetric Private Keys: E - Partition Symmetric Keys: E - USK: E - MTK: E
Import Public Key	This service is used to import public key,	Successful command response	Luna ICD command, session, object import	Luna ICD response, imported object handle	None	HSM Security Officer (SO) - Partition

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	certificate, domain object or data objects to a user partition.	e along with status as indicated in Table 3				Asymmetric Public Keys: R Crypto Officer (CO) - Partition Asymmetric Public Keys: R Crypto User (CU) - Partition Asymmetric Public Keys: R
Generate Random Data	This service for any user will return random data output from the DRBG.	Successful command response along with status as indicated in Table 3	Luna ICD command, request size	Luna ICD response, requested random data	Generate Random Data	Public User - DRBG_C: E - DRBG_V: E Crypto Officer (CO) - DRBG_C: E - DRBG_V: E Crypto User (CU) - DRBG_C: E - DRBG_V: E HSM Security Officer (SO) - DRBG_C: E - DRBG_V: E Audit Officer (AO) - DRBG_C: E - DRBG_V: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Reseed DRBG	This service for an authenticated user will reseed the DRBG with entropy.	Successful command response along with status as indicated in Table 3	Luna ICD command, session seed	Luna ICD response	Generate Random Data	HSM Security Officer (SO) - DRBG_C: G - DRBG_V: G - DRBG Seed : E - DRBG Entropy Input: E Crypto Officer (CO) - DRBG Seed : E - DRBG_C: G - DRBG_V: G - DRBG Entropy Input: E
Hash Digest	This service is used by a user to request a hash over a block of supplied data. N/A to Backup Config.	Successful command response along with status as indicated in Table 3	Luna ICD command, session algorithm, data hash	Luna ICD response, hash digest	Secure Hash	HSM Security Officer (SO) Crypto User (CU) Crypto Officer (CO)
Symmetric Encrypt/Decrypt	This service is used by a user to request encryption or decryption of a block of user-supplied data using	Successful command response along with status as indicated in Table 3	Luna ICD command, session, algorithm, algorithm parameters, key handle, data to en/decrypt	Luna ICD response, en/decrypted data	AES Symmetric Encryption/ Decryption AES Authenticated Symmetric Encryption/ Decryption TDES Symmetric	HSM Security Officer (SO) - Partition Symmetric Keys: E - SMK: E - MTK: E Crypto Officer (CO)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	a module stored cryptographic key. Output data resulting from the service is returned the user and not stored. N/A to Backup Confg.				Decryption (Legacy)	- Partition Symmetric Keys: E - USK: E - MTK: E Crypto User (CU) - Partition Symmetric Keys: E - USK: E - MTK: E
Sign (SigGen)	This service is used by a user to request a signature or MAC over a block of user supplied data using a module stored cryptographic key. The resulting signature from the operation is returned the user and not stored. N/A to Backup Config.	Successful command response along with status as indicated in Table 3	Luna ICD command, session, algorithm, algorithm parameter, data to sign	Luna ICD response, signature	RSA Signature Generation ECDSA Signature Generation LMS Signature Generation Cryptographic Message Authentication	HSM Security Officer (SO) - Partition Asymmetric Private Keys: E - Partition Symmetric Keys: E - SMK: E - MTK: E Crypto Officer (CO) - Partition Asymmetric Private Keys: E - Partition Symmetric Keys: E - USK: E - MTK: E Crypto User (CU) - Partition Asymmetric Private Keys: E - Partition Symmetric Keys: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- USK: E - MTK: E
Verify (SigVer)	This service is used by a user to request validation of a signature or MAC over a block of user-supplied data using a module stored cryptographic key. The service returns whether the validation was successful. N/A to Backup Config.	Successful command response along with status as indicated in Table 3	Luna ICD command, session, algorithm, algorithm parameter, data to verify signature	Luna ICD response	RSA Signature Verification ECDSA Signature Verification LMS Signature Verification Hash Message Authentication Cryptographic Message Authentication RSA Signature Verification (Legacy) ECDSA Signature Verification (Legacy)	HSM Security Officer (SO) - Partition Asymmetric Public Keys: E - Partition Symmetric Keys: E - SMK: E Crypto Officer (CO) - Partition Asymmetric Public Keys: E - Partition Symmetric Keys: E - USK: E Crypto User (CU) - Partition Asymmetric Public Keys: E - Partition Symmetric Keys: E - USK: E
Disable STM	This service disables Secure Transport Mode functionality at the request of the SO. The SRV is read from the SO Purple	Successful command response along with status as indicated in Table 3	Luna ICD command, session, SRV	Luna ICD response	Generate Random Data AES Symmetric Encryption/ Decryption KAS-ECC KTS-AES-HMAC Split Key Recover Key	HSM Security Officer (SO) - MTK: G - SRV: G,W,E - RDEK: G,E - RMAC: G,E - GSK: E - RPV: E - MTK_IS:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	PED key, the MTK is regenerated from the SRV and MTK_IS, and new MTK key splits are generated for the SRV and MTK_IS. The new SRV split is stored in internal Flash.					G,E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - Two-Step KDK: G,E,Z
Exit STM	This service exits Secure Transport Mode and restores the MTK at the request of the SO. The SRV is read from the SO Purple PED key and the MTK is regenerated from the SRV and MTK_IS.	Successful command response along with status as indicated in Table 3	Luna ICD command, SRV	Luna ICD response	KAS-ECC KTS-AES-HMAC Recover Key	HSM Security Officer (SO) - MTK: G - RDEK: G,E - RMAC: G,E - SRV: W,E - RPV: E - MTK_IS: E - EC Private Key: G,E,Z - EC Public Key : G,R,E,Z - EC Peer Public Key: W,E,Z - EC Shared Secret: G,E,Z - Two-Step KDK: G,E,Z

Table 13: Approved Services

All services listed in the table above can be accessed in Approved mode and non-Approved mode. The services listed here use the Security Functions in Section 2.6 and the Approved Algorithms in Section 2.5.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Generate Key	This service is used to generate symmetric keys or asymmetric key pairs requested by the end-user and stored in the corresponding cryptographic module partition for use or export. N/A to Backup Config.	DES Triple-DES RC2 RC4 RC5 CAST5 DILITHIUM (PQC) FALCON (PQC) RSA (non-compliant less than 112 bits of encryption strength) DSA ECDSA (non-compliant less than 112 bits of encryption strength) KYBER (PQC) SSL PRE-MASTER CAST3 ECDSA KeyGen (B and K curves)	HSM Security Officer (SO), Crypto Officer (CO)
Derive Key	This service is used to derive keys based on other key material stored in the module partition or supplied to it on request of the end-user. Derived keys are stored in the module partition for use or export. N/A to Backup Config.	ECDSA (non-compliant less than 112 bits of encryption strength) KYBER (PQC) Diffie-Hellman (key agreement; key establishment methodology; non-compliant less than 112 bits)	HSM Security Officer (SO), Crypto Officer (CO)
Wrap/Unwrap Key	This service is used to import or export user partition secret or private key objects using key wrapping as requested by the Crypto Officer. N/A to Backup Config.	RSA (key wrapping; key establishment methodology; non-compliant less than 112 bits of encryption strength)	HSM Security Officer (SO), Crypto Officer (CO), Crypto User (CU)

Name	Description	Algorithms	Role
Hash Digest	This service is used by a user to request a hash over a block of supplied data. N/A to Backup Config.	MD2 MD5 KECCAK	HSM Security Officer (SO), Crypto User (CU), Crypto Officer (CO)
Symmetric Encrypt/Decrypt	This service is used by a user to request encryption or decryption of a block of user-supplied data using a module stored cryptographic key. Output data resulting from the service is returned the user and not stored. N/A to Backup Config.	DES Triple-DES RC2 RC4 RC5 CAST5	HSM Security Officer (SO), Crypto Officer (CO), Crypto User (CU)
Sign (SigGen)	This service is used by a user to request a signature or MAC over a block of user supplied data using a module stored cryptographic key. The resulting signature from the operation is returned the user and not stored. N/A to Backup Config.	AES MAC (non-compliant) DES-MAC RC2-MAC RC5-MAC RIPEMD-160 CAST3-MAC CAST5-MAC SSL3-MD5-MAC SSL3-SHA1-MAC HMAC (non-compliant less than 112 bits of encryption strength) DILITHIUM (PQC) FALCON (PQC) RSA X-509 RSA (non-compliant less than 112 bits of encryption strength) DSA ECDSA (non-compliant less than 112 bits of encryption strength) RSA X9.31 RSA SigGen (sign using SHA-1 digest) ECDSA SigGen (sign using SHA-1 digest and B and K curves)	HSM Security Officer (SO), Crypto Officer (CO), Crypto User (CU)
Verify (SigVer)	This service is used by a user to request validation of a signature or MAC over a block of user-supplied data using a module stored cryptographic key. The	AES MAC (non-compliant) DES-MAC RC2-MAC RC5-MAC	HSM Security Officer (SO), Crypto Officer (CO),

Name	Description	Algorithms	Role
	service returns whether the validation was successful. N/A to Backup Config.	RIPEMD-160 CAST3-MAC CAST5-MAC SSL3-MD5-MAC SSL3-SHA1-MAC HMAC (non-compliant less than 112 bits of encryption strength) DILITHIUM (PQC) FALCON (PQC) RSA X-509 RSA (non-compliant less than 112 bits of encryption strength) ECDSA (non-compliant less than 112 bits of encryption strength)	Crypto User (CU)

Table 14: Non-Approved Services

The services listed in the table above using the Non-Approved, Not Allowed Algorithms listed in Table 6 cannot be accessed in Approved mode.

4.5 External Software/Firmware Loaded

The module does not allow external software to be loaded and executed inside its boundary except as part of the Firmware Update service.

Any firmware images that may be loaded as part of a Firmware Update must have been signed and verified by Thales TCT to ensure that the firmware will function correctly. This policy applies to initial firmware loading at manufacture and subsequent firmware updates.

The module only allows external software to be loaded inside its boundary as part of the Firmware Update service. Only properly formatted firmware may be loaded. The communication of initial or updated firmware to a target module shall be initiated by a Thales TCT module dedicated to that function. Firmware shall be digitally signed using the Thales TCT Firmware Signing Key and encrypted based upon the U2K. RSA (4096 bits) PKCS #1 V1.5 with SHA2-384 is used as the approved signature method. As part of the on-demand Firmware Update service, the Firmware Signing Certificate (FSC) is verified against the Root Certificate and is used to verify the signature of the delivered firmware image. The unencrypted firmware must not be visible outside a module before, during and after the loading operation.

5 Software/Firmware Security

5.1 Integrity Techniques

The Bootloader provides a SHA-1 integrity check (160-bit Error Detection Code (EDC)) of itself and a SHA2-256 integrity check (256-bit EDC) of the Firmware it loads on each power-on and reset cycle. The Bootloader begins by calculating the SHA-1 EDC of the Bootloader image and comparing the result to the expected value stored in Flash. If that Bootloader integrity check fails, the module will log an error message and halt.

Once the Bootloader verifies its own EDC, it then calculates the SHA2-256 EDC for the components of the Firmware image and compares the EDC to the expected value in Flash. If the Firmware integrity check fails, the Bootloader will log an error message and halt. On a successful Firmware integrity check, the Bootloader will proceed with loading and executing the Firmware.

5.2 Initiate on Demand

Bootloader and Firmware Integrity tests are performed as part of the pre-operational self-tests, which are executed when the module is initialized on power-up reset. The integrity tests can be invoked on demand by cycling power or resetting the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied :

The module supports a **limited operating environment** as defined in ISO/IEC 19790. The module Security Officer may update the module configuration to exit Approved mode as outlined in Section 2.4. The Security Officer may also initiate the Firmware Update service; the updated firmware would only be covered by this Security Policy if it were a firmware version specified in Section 2.4.

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 to determine if tamper attempts have been made.

Table 15: Mechanisms and Actions Required

The Luna M7 Cryptographic Module is a multi-chip embedded module as defined by FIPS 140-3 standard ISO/IEC 19790 section 7.7.1. The module is encased in a strong potted epoxy that provides tamper-evidence. Any tampering that might compromise a module's security is detectable by visual inspection of the physical integrity of a module. The HSM Security Officer should perform a visual inspection of the module at regular intervals.

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

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

7.2 Fault Induction Mitigation

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

The module will maintain its secure state in the event of data input / output failures. When data input / output capability is restored, the module will resume operation in the state it was prior to the input / output failure.

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.

7.3 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-8.27°C	EFP	The module needs to be returned to normal operating temperature range and reset to be able to use it.
HighTemperature	67.69°C	EFP	The module needs to be returned to normal operating temperature range and reset to be able to use it.
LowVoltage	4.106V	EFP	This condition results in system reset.
HighVoltage	5.805V	EFP	This condition results in system reset.

Table 16: 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 voltage, the module will reset itself and clear all working memory.

7.4 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-8.27 °C
HighTemperature	67.69 °C

Table 17: Hardness Testing Temperatures

7.5 Additional Information

Secure Transport Mode

The Luna M7 Cryptographic Module provides a Secure Transport Mode (STM) to ensure secure shipment of the module. This is done by deliberately erasing the module-level Master Tamper Key (MTK) under control of the SO. When the MTK is erased, all sensitive user partition key objects cannot be used, no user can login to the module, and no user cryptographic operations can occur. At the receiving site, the module can be put into operation under control of the SO by exiting Secure Transport Mode and restoring the MTK.

When the MTK is created, two key splits of the MTK are also created. One MTK split (MTK_IS) is held internal to the module. The other split, the Secure Recovery Vector (SRV), plays a critical role in Secure Transport Mode. When the SO issues the command to enable Secure Transport Mode (STM), the SRV split is transferred from the module to the SO Secure Recovery (Purple) PED Key. Another command zeroizes the MTK to prohibit user cryptographic operations. The only form of authentication available at this point is the provision of the SO Purple PED Key by the SO. When the module reaches its destination and the command to restore the MTK is issued, the SRV is read from the SO Purple PED Key and used with the internal split to reconstitute the MTK and re-enable user logins and cryptographic operations.

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Flash	256MB Flash	Static

Storage Area Name	Description	Persistence Type
RAM	2GB DDR3L RAM	Dynamic
NVRAM	4MB NVRAM	Static
RTC NVRAM	Battery backed RTC NVRAM	Static

Table 18: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
TPED_I	USB Host	RAM	Plaintext	Manual	Electronic	
TPED_O	RAM	USB Host	Plaintext	Manual	Electronic	
RPED_O	RAM	USB Target	Encrypted	Automated	Electronic	KAS-ECC
RPED_I	USB Target	RAM	Encrypted	Automated	Electronic	KAS-ECC
PIN_I	USB Target	RAM	Encrypted	Automated	Electronic	KTS-RSA
MFR_I	USB Target	RAM	Plaintext	N/A	Electronic	
ICD_I	USB Target	RAM	Plaintext	Automated	Electronic	
ICD_O	RAM	USB Target	Plaintext	Automated	Electronic	
WICD_I	USB Target	RAM	Encrypted	Automated	Electronic	KTS-AES
WICD_O	RAM	USB Target	Encrypted	Automated	Electronic	KTS-AES

Table 19: SSP Input-Output Methods

Note that there are additional Security Functions involved in the Remote PED secure channel that is used for the RPED_I and RPED_O SSP Input and Output Methods. As noted in Section 3.2, the ECC Key Agreement Scheme generates the key material that is used by the AES HMAC Wrap/Unwrap Key Security Function, which uses AES Symmetric Encryption/Decryption (AES-256-CBC) and Hash Message Authentication (HMAC-SHA2-256) to implement the SP800-38F compliant tunnel for transferring key material across this interface.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
ZM1	Power-on reset initialization including read/write test and clearing of all RAM space	Zeroized by power cycle or module reset	Yes
ZM2	Erasure of MTK in Nonvolatile RAM	Zeroize MTK (Tamper) ICD command to place module in Secure Transport Mode	Yes
ZM4	Execution of firmware zeroize function that deletes all user cryptographic objects stored in nonvolatile module memory and deletes all user keys (USK, SMK) and partitions. The module is in its	Zeroized via ICD command, Zeroized when moving to/from FIPS 140-3 Approved mode and non-Approved mode of operation, Zeroized when the configured threshold for	Yes

Zeroization Method	Description	Rationale	Operator Initiation
	factory reset state and must be re-initialized	failed SO login attempts is reached	
ZM5	Remanufacturing zeroization that clears all Flash and nonvolatile memory devices except for bootloader space	All SSPs in Static storage areas are zeroized	No
ZM6	Zeroized following use	RAM memory where SSP was stored is zeroized following the operation that used the SSP	Yes

Table 20: SSP Zeroization Methods

ZM5 is a wipe of all nonvolatile memory space that is intended to put the module in its original factory manufacturing state. A signed firmware image from Thales TCT that is dedicated to the task of erasing all nonvolatile memory is required to perform ZM5.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Challenge Secret	Used in PED Key plus Challenge Secret Authentication mode. 16-byte random string generated by the cryptographic module, masked to printable characters, and output via the PED display when the user is created. It is input by the operator as additional authentication data for a client application login.	128-512 bits - 75-315 bits	Authentication - CSP	Generate Random Data		
Random Challenge	Used in PED Key plus Challenge Secret Authentication mode. A one-time random number generated by the cryptographic module and sent to the calling application for each login. It is combined with the input Challenge Secret to compute the one-time response that is returned to the cryptographic module	384 bits - 384 bits	Authentication - PSP	Generate Random Data		
Challenge Response	A 20-byte value used for authentication in the challenge response scheme. It is generated	160 bits - 160 bits	Authentication - PSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	using the challenge secret and the one-time random challenge value.					
PED Key Authentication Data	Used in PED Key Authentication modes. A 48-byte random value that is generated by the module when the SO or User is created. It is written out to the serial memory device (PED Key) via the Trusted Channel. It is input from the PED Key as part of Login command	384 bits - 384 bits	Authentication - CSP	Generate Random Data		
User Password	Used in Password Authentication mode. User provided 8-255 character string that is input as part of the Login command. It is input encrypted under the PEC and using KTS-OAEP-basic and uses PBKDF to generate the PIN Storage Key.	64-2040 bits - N/A	Authentication - CSP		KTS-RSA	Password Based KDF
PSK	PIN Storage Key (PSK): Key that encrypts the SO and partition User storage keys.	256 bits - 256 bits	Symmetric, AES CBC - CSP		Password Based KDF	AES Symmetric Encryption/ Decryption
KCV	Cloning Domain Vector / Key Cloning Vector (KCV): 48-byte value that is used to control a module's ability to participate in the	384 bits - 384 bits	Generic Secret - PSP			KAS-IFC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	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.					
USK	User Storage Key (USK): This key is used to encrypt all sensitive attributes of all private objects owned by the User. Encrypted, as part of the UAV, by the key taken from the PED Key data.	256 bits - 256 bits	Symmetric, AES-ECB - CSP	Generate Random Data		AES Symmetric Encryption/ Decryption
SMK	Security Officer Master Key (SMK): The storage key for the SO. This key is used to encrypt all sensitive attributes of all private objects owned by the SO. The USK/SMK is stored encrypted by an AES key derived from the User/SO PED Key Authentication data.	256 bits - 256 bits	Symmetric, AES-ECB - CSP			AES Symmetric Encryption/ Decryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
GSK	Global Storage Key (GSK): 32-byte AES key that is the same for all users on a specific Luna cryptographic module. It is used to encrypt permanent parameters within the non-volatile memory area reserved for use by the module.	256 bits - 256 bits	Symmetric, AES-ECB - CSP			AES Symmetric Encryption/ Decryption
SGSK	Secondary Global Storage Key (SGSK): It is used to encrypt non permanent parameters - parameters re-generated for every module initialization.	256 bits - 256 bits	Symmetric, AES-ECB - CSP	Generate Random Data		AES Symmetric Encryption/ Decryption
TUK	Token or Module Unwrapping Key (TUK): Current version (v4) of the 4096-bit RSA private key used in the cloning protocol for FIPS mode. It is generated on power up if it does not exist.	4096 bits - 150 bits	Private, RSA-4096 - CSP	RSA Key Pair Generation		KAS-IFC
TWC	Token or Module Wrapping Certificate (TWC): Current version (v4) of the public key certificate used in the KAS2-basic Key Agreement Scheme for the session encryption key as part of the cloning protocol in FIPS mode. It is	4096 bits - 150 bits	Public, RSA-4096 - PSP	RSA Key Pair Generation		KAS-IFC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	generated on power up and signed by the HOK.					
PEK	Password Encryption Key (PEK): A 4096 bit RSA private key used to decrypt user passwords that are provided to the module. It is generated on power up if it does not exist.	4096 bits - 150 bits	Private, RSA-4096 - CSP	RSA Key Pair Generation		KTS-RSA
PEC	Password Encryption Certificate (PEC): The X.509 public key certificate corresponding to the PEK. The PEC is provided to the host as part of the KTS-OAEP-Basic scheme for secure transport of password data. It is generated on power-up and signed by the HOK.	4096 bits - 150 bits	Public, RSA 4096 - PSP	RSA Key Pair Generation		KTS-RSA
U2K	U2 Key: 24-byte generic secret key loaded at manufacturing and used as shared secret to derive product specific keys	192 bits - 192 bits	Generic Secret - CSP			KAS Key Derivation Algorithm
TVK	Token or Module Variable Key (TVK): It is used to encrypt cached User authentication data when auto-activation is enabled.	256 bits - 256 bits	Symmetric, AES-ECB - CSP			AES Symmetric Encryption/ Decryption
MTK	Master Tamper Key (MTK): The MTK encrypts all sensitive values for use in the cryptographic	256 bits - 256 bits	Symmetric, AES-ECB - CSP	Generate Random Data		AES Symmetric Encryption/ Decryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	accelerators. The MTK in non-volatile RAM is actively zeroized in response to a User command.					
ROOT	Root Certificate (ROOT): The X.509 public key certificate corresponding to the Thales TCT Root signing key. It is self-signed. Used in verifying Manufacturing Integrity, Firmware, and License Signing Certificates (MIC, FSC, and LSC).	4096 bits - 150 bits	Public, RSA 4096 - PSP			RSA Signature Verification RSA Signature Verification (Legacy)
MIC	Manufacturer's Integrity Certificate (MIC): Used in verifying Hardware Origin Certificates (HOCs), which are generated in response to a customer function call to provide proof of hardware origin. It is signed by the Root Key.	4096 bits - 150 bits	Public, RSA 4096 - PSP			RSA Signature Verification RSA Signature Verification (Legacy)
FSC	Firmware Signing Certificate (FSC): The X.509 public key certificate corresponding to the Firmware Signing Key (FSK). It is input in plaintext as part of the Firmware Update File (FUF). It is signed by the Thales TCT Root signing	4096 bits - 150 bits	Public, RSA 4096 - PSP			RSA Signature Verification RSA Signature Verification (Legacy)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	key. Used to verify Firmware images on initial load.					
LSC	License Signing Certificate (LSC): The X.509 public key certificate corresponding to the License Signing Key (LSK). It is input in plaintext as part of the Configuration Update File (CUF). It is signed by the Thales TCT Root signing key. Used to verify Configuration Update images on initial load.	4096 bits - 150 bits	Public, RSA 4096 - PSP			RSA Signature Verification RSA Signature Verification (Legacy)
CITS-DAK	Device Authentication Key (CITS-DAK): 4096-bit RSA private key used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module. It is generated upon first request.	4096 bits - 150 bits	Private, RSA 4096 - CSP	RSA Key Pair Generation		RSA Signature Generation
CITS-DAC	Device Authentication Certificate (CITS-DAC): The X.509 public key certificate corresponding to the CITS-DAK. It is signed by the HOK. Used for a specific PKI implementation requiring	4096 bits - 150 bits	Public, RSA 4096 - PSP	RSA Key Pair Generation		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	assurance that a key or a specific action originated within the hardware crypto module.					
HOK	Hardware Origin Key (HOK): RSA private key used to sign certificates for other device messaging key pairs, such as the TWC. It is generated at the time the device is manufactured.	4096 bits - 150 bits	Private, RSA 4096 - CSP	RSA Key Pair Generation		RSA Signature Generation
HOC	Hardware Origin Certificate (HOC): The X.509 public key certificate corresponding to the HOK. It is signed by the Manufacturer's Integrity Key (MIK) at the time the device is manufactured.	4096 bits - 150 bits	Public, RSA 4096 - PSP	RSA Key Pair Generation		
RPV	Remote PED Vector (RPV): A randomly generated 256-bit secret, which must be shared between a Remote PED and a cryptographic module in order to establish a secure communication channel between them.	256 bits - 256 bits	Generic Secret - PSP	Generate Random Data		KAS-ECC
SRV	Secure Recovery Vector (SRV): A split of the MTK that is stored encrypted in Flash by default. It is	256 bits - 256 bits	Generic Secret - CSP	Generate Random Data		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	written to the Purple PED Key when Secure Transport Mode (STM) is enabled. The SRV and the MTK_IS splits are combined to regenerate the MTK after it has been zeroized.					
DRBG_C	Hash_DRBG Constant state variable, dependent upon the entropy DRBG Seed, that is stored ephemerally in unreadable RNG register space and updated on each Instantiate and Reseed operation in accordance with NIST SP 800-90A.	440 bits - 440 bits	DRBG State - CSP	Hash DRBG (A5022)		Generate Random Data Cryptographic Key Generation
DRBG_V	Hash_DRBG Value state variable that is stored ephemerally in unreadable RNG register space and updated on each Instantiate, Generate, and Reseed operation in accordance with NIST SP 800-90A.	440 bits - 440 bits	DRBG State - CSP	Hash DRBG (A5022)		Generate Random Data Cryptographic Key Generation
SALK	Secure Audit Logging Key (SALK): A 256-bit SHA2 HMAC key used to verify data integrity and authentication of the log messages. Saved in the	256 bits - 256 bits	Authentication, HMAC-SHA2-256 - CSP	Generate Random Data	KTS-AES	Hash Message Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	parameter area of Flash memory.					
SADK	Secure Audit Domain Key (SADK): A 256-bit 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 bits - 128 bits	Symmetric, AES-KWP - CSP		KAS Key Derivation Algorithm	KTS-AES
RDEK	Remote PED session Data Encryption Key (RDEK): 256-bit AES key established and used to encrypt RPED tunnel across command interface to Remote PED.	256 bits - 128 bits	Symmetric, AES CBC - CSP		KAS-ECC	AES Symmetric Encryption/ Decryption
RMAC	Remote PED session Message Authentication Code Key (RMAC): HMAC-SHA-256 key established and used to authenticate RPED tunnel across command interface to Remote PED.	256 bits - 128 bits	Authentication, HMAC SHA 256 - CSP		KAS-ECC	Hash Message Authentication
CKEV	Cloning Key Encryption Vector (CKEV): 256-bit AES key established by KAS2-basic and used to AES-KWP wrap and unwrap partition cryptographic objects for Cloning	256 bits - 128 bits	Symmetric, AES KWP - CSP		KAS-IFC	KTS-AES

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Partition Asymmetric Public Keys	Asymmetric Key Pairs (Public Keys for a User partition or session): RSA, ECDSA, LMS, DSA. In Backup Config, User Partition Keys are Established but not Generated.	RSA: 2048-4096 bits ECDSA: 224-521 bits LMS: 416-512 bits DSA: 2048-3072 - RSA: 112- 150 bits ECDSA: 112-256 bits LMS: 192-256 bits DSA: 112-128 bits	Asymmetric, RSA, ECDSA, LMS, DSA - PSP	RSA Key Pair Generation ECDSA Key Generation LMS Key Pair Generation	KTS-AES	RSA Signature Generation RSA Signature Verification ECDSA Signature Generation ECDSA Signature Verification DSA Signature Verification (Legacy) LMS Signature Generation LMS Signature Verification RSA Signature Verification (Legacy)
Partition Symmetric Keys	Symmetric Keys (for a User partition or session): AES, Generic, Triple-Des. In Backup Config. User Partition Keys are Established but not Generated.	AES: 128-256 bits Generic: 128-4096 bits Triple-Des: 192 bits - AES: 128-256 bits Generic: 128-256 bits Triple-DES: 112 bits	Symmetric, AES, Generic, Triple-DES - CSP	Cryptographic Key Generation	KTS-AES	AES Symmetric Encryption/ Decryption AES Authenticated Symmetric Encryption/ Decryption TDES Symmetric Decryption (Legacy) Hash Message Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Cryptographic Message Authentication KTS-AES KAS Key Derivation Algorithm Key-Based KDF
DRBG Seed	Hash_DRBG seed material consisting of 256-bit DRBG Entropy Input with appended 128-bit Nonce from ENT ESV (#E97) approved module noise source.	384 bits - 192 bits	DRBG Seed - CSP	Hash DRBG (A5022)		Generate Random Data
Partition Asymmetric Private Keys	Asymmetric Key Pairs (Private Keys for a User partition or session): RSA, ECDSA, LMS. In Backup Config. User Partition Keys are Established but not Generated.	RSA: 2048-4096 bits ECDSA: 224-521 bits LMS: 416-512 bits - RSA: 112- 150 bits ECDSA: 112- 256 bits LMS: 192-256 bits	Asymmetric, RSA, ECDSA, LMS - CSP	RSA Key Pair Generation LMS Key Pair Generation	KTS-AES	RSA Signature Generation ECDSA Signature Generation LMS Signature Generation
MTK_IS	MTK Internal Split (MTK_IS): A split of the MTK that is stored in Flash. The MTK_IS and the SRV splits are combined to regenerate the MTK after it has been zeroized.	256 bits - 256 bits	Generic Secret - CSP	Generate Random Data		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Hash_DRBG 256-bit Entropy Input taken from ESV (#E97) approved module noise source.	256 bits - 192 bits	DRBG Entropy Input - CSP	ESV noise source		Generate Random Data
Two-Step KDK	Key Derivation Key (KDK) output of first step (Randomness Extraction) of SP 800-56Cr2 Two-Step Key Derivation Function	128-bits - 128-bits	Symmetric, AES - CSP		KAS Key Derivation Algorithm	Key-Based KDF
EC Private Key	Local ephemeral private key used in ECC Key agreement (P-384)	384-bits - 192-bits	Asymmetric, ECDSA - CSP	ECDSA Key Generation		KAS-ECC
EC Public Key	Local ephemeral public key used in ECC Key agreement (P-384)	384-bits - 192-bits	Asymmetric, ECDSA - PSP	ECDSA Key Generation		KAS-ECC
EC Peer Public Key	Imported ephemeral public key used in ECC Key agreement (P-384)	384-bits - 192-bits	Asymmetric, ECDSA - PSP			KAS-ECC
EC Shared Secret	Shared secret established by ECC key agreement (P-384)	384 bits - 192 bits	Shared Secret - CSP		KAS-ECC	KAS Key Derivation Algorithm
RSA Peer Public Key	Imported ephemeral public key used in RSA Key Agreement Scheme (RSA-4096)	4092 bits - 150 bits	Asymmetric, RSA - PSP			KAS-IFC
RSA Shared Secret	Shared secret established by KAS2 key agreement (RSA-4096, concatenated)	8192 bits - 256 bits	Shared Secret - CSP		KAS-IFC	KAS Key Derivation Algorithm

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Challenge Secret	TPED_O RPED_O	Flash:Encrypted	During generation and transmission and while processing Login	ZM4 ZM5	SGSK:Encrypted by SGSK RDEK:Encrypted by RDEK RMAC:Authenticated by RMAC
Random Challenge	ICD_O	RAM:Plaintext	During generation and transmission and while processing Login	ZM1 ZM6	Challenge Secret:XORed with Challenge Secret
Challenge Response	ICD_I	RAM:Plaintext	While processing Login	ZM1	Challenge Secret:Derived From Random Challenge:Derived From
PED Key Authentication Data	TPED_I TPED_O RPED_O RPED_I	RAM:Plaintext Flash:Encrypted	During generation and transmission and while processing Login	ZM1 ZM4 ZM5	PSK:Establishes PSK RDEK:Encrypted by RDEK RMAC:Authenticated by RMAC TVK:Encrypted by TVK
User Password	PIN_I	RAM:Plaintext	While processing Login	ZM1 ZM6	PSK:Establishes PSK PEC:Wrapped By PEC
PSK	TPED_I TPED_O	RAM:Plaintext	While processing Login	ZM1 ZM6	USK:Encrypts SMK:Encrypts PED Key Authentication Data:Established by PED Key Authentication Data User Password:Established by User Password
KCV	TPED_I TPED_O RPED_O RPED_I	Flash:Encrypted	During generation, transmission, and key establishment	ZM4 ZM5	RDEK:Encrypted By RMAC:Authenticated By SADK:Establishes CKEV:Establishes USK:Encrypted By SMK:Encrypted By Two-Step KDK:Establishes

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
USK		Flash:Encrypted RAM:Plaintext	During generation and while login session is active	ZM1 ZM4 ZM5	PSK:Encrypted by PSK GSK:Encrypts SGSK:Encrypts KCV:Encrypts
SMK		Flash:Encrypted RAM:Plaintext	During generation and while login session is active	ZM1 ZM4 ZM5	PSK:Encrypted by PSK GSK:Encrypts SGSK:Encrypts KCV:Encrypts
GSK	MFR_I	Flash:Encrypted RAM:Plaintext	While login session is active	ZM1 ZM5	USK:Encrypted by USK SMK:Encrypted by SMK TUK:Encrypts HOK:Encrypts U2K:Encrypts SRV:Encrypts
SGSK		Flash:Encrypted RAM:Plaintext	While login session is active	ZM1 ZM4 ZM5	USK:Encrypted by USK SMK:Encrypted by SMK Challenge Secret:Encrypts
TUK		Flash:Encrypted RAM:Plaintext	During generation and Cloning service	ZM1 ZM5	GSK:Encrypted by GSK TWC:Paired With RSA Shared Secret:Establishes CKEV:Establishes
TWC	ICD_O	RAM:Plaintext	Stored in RAM on power up until reset	ZM1	HOK:Signed by HOK TUK:Paired With RSA Shared Secret:Establishes CKEV:Establishes
PEK		RAM:Plaintext Flash:Plaintext	While processing Login	ZM1	PEC:Paired With
PEC	ICD_O	RAM:Plaintext Flash:Plaintext	While processing Login	ZM1	PEK:Paired With HOK:Signed by HOK
U2K	MFR_I	Flash:Encrypted RAM:Plaintext	During firmware update and log secret encryption	ZM1 ZM5 ZM6	GSK:Encrypted by GSK SADK:Establishes SADK Two-Step KDK:Establishes

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TVK		RTC NVRAM:Plaintext	During generation and when used for encryption	ZM4 ZM5	PED Key Authentication Data:Encrypts
MTK		NVRAM:Plaintext	During generation, establishment, and when used for encryption	ZM2 ZM5	Partition Asymmetric Public Keys:Encrypts Partition Asymmetric Private Keys:Encrypts Partition Symmetric Keys:Encrypts SRV:Generated by combining SRV, MTK_IS
ROOT	MFR_I ICD_O	Flash:Encrypted RAM:Plaintext	During transmission and certificate verification	ZM1 ZM5	MIC:Verifies MIC FSC:Verifies FSC LSC:Verifies LSC
MIC	MFR_I ICD_O	Flash:Encrypted RAM:Plaintext	During transmission and certificate verification	ZM1 ZM5	ROOT:Verified by ROOT HOC:Verifies HOC
FSC	ICD_I	RAM:Plaintext	During Firmware Update service	ZM1	ROOT:Verified by ROOT
LSC	ICD_I	RAM:Plaintext	During Configuration Update service	ZM1	ROOT:Verified by ROOT
CITS-DAK		Flash:Encrypted RAM:Plaintext		ZM1 ZM5	GSK:Encrypted by GSK CITS-DAC:Paired With
CITS-DAC	ICD_O	RAM:Plaintext	When used for signing	ZM1	CITS-DAK:Paired With HOK:Signed by HOK
HOK		Flash:Encrypted RAM:Plaintext	Stored in RAM on power-up until reset	ZM1 ZM5	HOC:Paired With GSK:Encrypted by GSK TWC: Signs TWC PEC: Signs PEC CITS-DAC: Signs CITS-DAC
HOC	MFR_I ICD_O	Flash:Encrypted	During transmission and certificate verification	ZM5	HOK:Paired With MIC:Verified by MIC TWC:Verifies TWC PEC:Verifies PEC CITS-DAC:Verifies CITS DAC

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RPV	TPED_I TPED_O	Flash:Encrypted RAM:Plaintext	During transmission and Remote PED tunnel establishment	ZM1 ZM4 ZM5	RDEK:Establishes RDEK RMAC:Establishes RMAC
SRV	TPED_I TPED_O RPED_O RPED_I	Flash:Encrypted RAM:Plaintext	During transmission and STM transitions	ZM1 ZM4 ZM5	MTK:Regenerates MTK with MTK_IS GSK:Encrypts
DRBG_C		RAM:Plaintext	Stored in hardware DRBG until reset	ZM1	DRBG Seed :Established By
DRBG_V		RAM:Plaintext	Stored in hardware DRBG until reset	ZM1	DRBG Seed :Established By
SALK	WICD_I WICD_O	Flash:Plaintext	Stored in RAM on power up until reset	ZM1 ZM5	SADK:Wrapped by SADK
SADK		Flash:Plaintext	During log secret import and export	ZM1 ZM6	SALK:Wraps SALK U2K:Established by U2K KCV:Established by KCV Two-Step KDK:Established By
RDEK		RAM:Plaintext	During use of Remote PED tunnel	ZM1 ZM6	RPV:Established by RPV EC Private Key:Established By EC Public Key :Established By EC Peer Public Key:Established By EC Shared Secret:Established By Two-Step KDK:Established By
RMAC		RAM:Plaintext	During use of Remote PED tunnel	ZM1 ZM6	RPV:Established by RPV EC Private Key:Established By EC Public Key :Established By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					EC Peer Public Key:Established By EC Shared Secret:Established By Two-Step KDK:Established By
CKEV		RAM:Plaintext	During Cloning service	ZM1	KCV:Established by KCV TUK:Established By TWC:Established By RSA Peer Public Key:Established By RSA Shared Secret:Established By Two-Step KDK:Established By
Partition Asymmetric Public Keys	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted	Session Partition Keys exist in RAM until the Partition user logs out.	ZM1 ZM4 ZM5	SMK:Encrypted By USK:Encrypted By MTK:Encrypted By CKEV:Wrapped By Partition Symmetric Keys:Wrapped By
Partition Symmetric Keys	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted	Session Partition Keys exist in RAM until the Partition user logs out.	ZM1 ZM4 ZM5	SMK:Encrypted By USK:Encrypted By MTK:Encrypted By CKEV:Wrapped By Partition Symmetric Keys:Wrapped By
DRBG Seed		RAM:Plaintext	Temporary storage in hardware DRBG during Instantiate or Reseed, loaded directly from noise source	ZM1	DRBG_C:Establishes DRBG_V:Establishes
Partition Asymmetric Private Keys	WICD_I WICD_O	Flash:Encrypted RAM:Encrypted	Session Partition Keys exist in RAM until the Partition user logs out.	ZM1 ZM4 ZM5	SMK:Encrypted By USK:Encrypted By MTK:Encrypted By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					CKEV:Wrapped By Partition Symmetric Keys:Wrapped By
MTK_IS		Flash:Plaintext	During STM transitions	ZM5	MTK:Regenerates MTK with SRV
DRBG Entropy Input		RAM:Plaintext	Temporary storage in hardware DRBG during Instantiate or Reseed, loaded directly from noise source	ZM1	
Two-Step KDK		RAM:Plaintext	Temporary storage after Randomness Extraction before Key Expansion during SP 800-56Cr2 Two-Step Key Derivation Function	ZM1 ZM6	EC Shared Secret:Established By RSA Shared Secret:Established By U2K:Established By KCV:Established By SADK:Establishes RDEK:Establishes RMAC:Establishes CKEV:Establishes
EC Private Key		RAM:Plaintext	Temporary storage during SP800-56Ar3 ECC Key Agreement Scheme	ZM1 ZM6	EC Public Key :Paired With EC Shared Secret:Establishes
EC Public Key	ICD_O	RAM:Plaintext	Temporary storage during SP800-56Ar3 ECC Key Agreement Scheme	ZM1 ZM6	EC Private Key:Paired With EC Shared Secret:Establishes
EC Peer Public Key	ICD_I	RAM:Plaintext	Temporary storage during SP800-56Ar3 ECC Key Agreement Scheme	ZM1 ZM6	EC Shared Secret:Establishes
EC Shared Secret		RAM:Plaintext	Temporary storage during SP800-56Ar3 ECC Key Agreement Scheme	ZM1 ZM6	Two-Step KDK:Establishes EC Private Key:Established By EC Public Key :Established By

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					EC Peer Public Key:Established By
RSA Peer Public Key	ICD_I	RAM:Plaintext	Temporary storage during SP800-56Br2 RSA Key Agreement Scheme	ZM1 ZM6	RSA Shared Secret:Establishes
RSA Shared Secret		RAM:Plaintext	Temporary storage during SP800-56Br2 RSA Key Agreement Scheme	ZM1 ZM6	Two-Step KDK:Establishes TUK:Established By TWC:Established By RSA Peer Public Key:Established By

Table 22: SSP Table 2

9.5 Transitions

The SHA-1 algorithm as implemented by the module will be non-approved for all purposes, starting January 1, 2031.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
EDC (160 bits)	SHA-1 Integrity Check	KAT	SW/FW Integrity	Log message, Module halt on failure, Boot on success	Bootloader performs a SHA-1 integrity check of bootloader image
EDC (256 bits)	SHA2-256 Integrity Check	KAT	SW/FW Integrity	Log message, Module halt on failure, Boot on success	Bootloader performs a SHA2-256 integrity check of firmware image

Table 23: Pre-Operational Self-Tests

The module provides self-tests on power-up to confirm the firmware integrity of the bootloader itself and of all components of the firmware image launched by the bootloader. The loaded firmware image checks the random number generator and each of the approved cryptographic algorithms by running the complete suite of its Continuous Algorithm Self-Tests (CAST) as part of the power-on sequence. All interfaces and external operations are disabled until the Pre-Operational Self-Tests and CASTs complete successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ESV (Entropy Certificate #E97)	SP800-90B CRNGT Health Tests	CRNGT	CAST	Function Fail / Error Logged	CRNGT Statistical Tests	Per Entropy Sample
RSA KeyGen (FIPS186-5) (A5022)	RSA Pairwise Consistency Sign / Verify Test, all key sizes	PCT	PCT	Function Fail	RSA Sign / Verify using generated keypair	Per Operation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-5) (A5022)	ECDSA Pairwise Consistency Sign / Verify Test, all key sizes	PCT	PCT	Function Fail	ECDSA Sign / Verify using generated keypair	Per Operation
Firmware Load Test	RSA SigVer (FIPS186-4), 4096-bit modulus, SHA2-384 hash	Signature Verification	SW/FW Load	Function Fail / Error Logged, Module will continue executing with existing firmware	RSA SigVer performed on input firmware image	Per Operation
AES-CBC (A5021)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-CFB128 (A5021)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-CFB8 (A5021)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module	Encrypt, Decrypt	Power On, Request

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				halt on failure		, Periodic
AES-CMAC (A5021)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-CTR (A5021)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-ECB (A5021)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-OFB (A5021)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
DSA SigVer (FIPS186-4) (A5021)	L=1024, SHA 1; L=2048, SHA2 224	KAT	CAST	Log message, Module halt on failure	Verify	Power On, Request, Periodic
ECDSA SigGen (FIPS186-5) (A5022)	Curve: P-256 Hash: SHA2-256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
ECDSA SigVer (A5021)	Curve: P-256 Hash: SHA2-256	KAT	CAST	Log message,	Verify	Power On,

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Module halt on failure		Request, Periodic
HMAC-SHA2-224 (A5021)	MAC: 224 Key Length: 1048	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA2-256 (A5021)	MAC: 256 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA2-384 (A5021)	MAC: 384 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA2-512 (A5021)	MAC: 512 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA3-224 (A5021)	MAC: 224 Key Length: 32,160,1176	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA3-256 (A5021)	MAC: 256 Key Length: 32,160,1176	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-384 (A5021)	MAC: 384 Key Length: 32,160,1176	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA3-512 (A5021)	MAC: 512 Key Length: 32,160,1176	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
KAS-ECC-SSC Sp800-56Ar3 (A5021)	Curve: P-384 Scheme: ephemeralUnified KAS Role: Initiator, Responder	KAT	CAST	Log message, Module halt on failure	Initiator, Responder	Power On, Request, Periodic
KAS-IFC-SSC (A5021)	Scheme: KAS2 KAS Role: Initiator,Responder; KeyGenerationMethod: rsakpg2-basic; Modulo: 2048,4096; HashFunctionZ: SHA2-512	KAT	CAST	Log message, Module halt on failure	Initiator, Responder	Power On, Request, Periodic
KDA TwoStep SP800-56Cr2 (A5021)	L: 2048 SaltLen: 128, FixedInfoPattern: "label||algorithmId||uPartyInfo||vPartyInfo" FixedInfoEncoding: Concatenation KDF Mode: Counter MAC: CMAC-AES128 CounterLoc: "before fixed data" CounterLen: 32, IV Len: 0 zLength: 496, 2192	KAT	CAST	Log message, Module halt on failure	KDA	Power On, Request, Periodic
KDF SP800-108 (A5021)	PRF: CMAC_AES128 CounterLoc: Before Fixed Data CounterLen: 32 COUNT=0 FixedInputLen: 72 L: 360,1024	KAT	CAST	Log message, Module halt on failure	KBKDF	Power On, Request, Periodic
KTS-IFC (A5021)	Scheme: KTS-OAEP-basic KAS Role: Responder KeyGenMethod: rsakpg1-	KAT	CAST	Log message,	Responder	Power On,

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	basic Modulo: 4096 FixedPubExp: 010001 L: 512 Hash: SHA2-512			Module halt on failure		Request, Periodic
LMS KeyGen (A5021)	LMS Mode: LMS_SHA256_M24_H5, LMS_SHA256_M32_H5 LMOTS Mode: LMOTS_SHA256_N24_W4, LMOTS_SHA256_N32_W8	KAT	CAST	Log message, Module halt on failure	KeyGen	Power On, Request, Periodic
LMS SigGen (A5021)	LMS Mode: LMS_SHA256_M24_H5, LMS_SHA256_M32_H5 LMOTS Mode: LMOTS_SHA256_N24_W2, LMOTS_SHA256_N32_W1	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
LMS SigVer (A5021)	LMS_SHA256_M24_H15,LMS_SHA256_M24_H10,LMS_SHA256_M24_H20,LMS_SHA256_M24_H5,LMS_SHA256_M24_H25,LMS_SHA256_M32_H15,LMS_SHA256_M32_H25,LMS_SHA256_M32_H10,LMS_SHA256_M32_H20,LMS_SHA256_M32_H5 LMOTS Mode: LMOTS_SHA256_N24_W8,LMOTS_SHA256_N24_W1,LMOTS_SHA256_N24_W2,LMOTS_SHA256_N24_W4,LMOTS_SHA256_N32_W8,LMOTS_SHA256_N32_W1,LMOTS_SHA256_N32_W2,LMOTS_SHA256_N32_W4	KAT	CAST	Log message, Module halt on failure	Verify	Power On, Request, Periodic
PBKDF (A5021)	HMAC Algs: SHA-1,SHA2-224,SHA2-256,SHA2-384,SHA2-512 Key Lengths: 1792,800,1392,272,1744 Iteration Count: 764,26,408,10,437	KAT	CAST	Log message, Module halt on failure	PBKDF	Power On, Request, Periodic
RSA Decryption Primitive (A5021)	Modulo: 2048	KAT	CAST	Log message, Module	Decrypt	Power On, Request

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				halt on failure		, Periodic
RSA SigVer (FIPS186-4) (A5021)	Modulo: 2048 Hash: SHA2 256	KAT	CAST	Log message, Module halt on failure	Verify	Power On, Request, Periodic
SHA-1 (A5021)	Msg Len: 640 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-224 (A5021)	Msg Len: 448 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-256 (A5021)	Msg Len: 448 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-384 (A5021)	Msg Len: 896 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-512 (A5021)	Msg Len: 896 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA3-224 (A5021)	Msg Len: 0, 56 bits	KAT	CAST	Log message,	Hash	Power On,

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Module halt on failure		Request, Periodic
SHA3-256 (A5021)	Msg Len: 0, 96 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA3-384 (A5021)	Msg Len: 0, 104 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA3-512 (A5021)	Msg Len: 0, 152 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
TDES-CBC (A5021)	Keying Option: 2 Key Length: 192	KAT	CAST	Log message, Module halt on failure	Decrypt	Power On, Request, Periodic
AES-CBC (A5022)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-CFB128 (A5022)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CFB8 (A5022)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-CMAC (A5022)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-CTR (A5022)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-ECB (A5022)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-GCM (A5022)	Key Length: 128, 192, 256 Tag Length: 128 IV Length: 96 Payload Length: 8, 128, 480, 512, 1020 AAD Length: 8, 128, 160, 512	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-GMAC (A5022)	Key Length: 128 Tag Length: 128 IV Length: 96 AAD Length: 128	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-KW (A5022)	Key Length: 128, 192, 256 Payload Length: 128, 192, 256	KAT	CAST	Log message, Module	Encrypt, Decrypt	Power On, Request

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				halt on failure		, Periodic
AES-KWP (A5022)	Key Length: 128, 192, 256 Payload Length: 8, 64, 72	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-OFB (A5022)	Key Length: 128, 192, 256	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
AES-XTS Testing Revision 2.0 (A5022)	Key Length: 128, 256 Payload Length: 136, 256, 4096	KAT	CAST	Log message, Module halt on failure	Encrypt, Decrypt	Power On, Request, Periodic
DSA SigVer (FIPS186-4) (A5022)	L=1024, SHA 1 L=2048, SHA2 224	KAT	CAST	Log message, Module halt on failure	Verify	Power On, Request, Periodic
ECDSA SigVer (A5022)	Curve: P-256 Hash: SHA2-256	KAT	CAST	Log message, Module halt on failure	Verify	Power On, Request, Periodic
Hash DRBG (A5022)	SHA-256 PredictionResistance = False EntropyInputLen = 256 NonceLen = 128 PersonalizationStringLen = 0 AdditionalInputLen = 0, 256 ReturnedBitsLen = 1024	KAT	CAST	Log message, Module halt on failure	instantiate, Reseed, Generate, Unins	Power On, Request, Periodic

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					tantiate	
HMAC-SHA2-224 (A5022)	MAC: 224 Key Length: 1048	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA2-256 (A5022)	MAC: 256 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA2-384 (A5022)	MAC: 384 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA2-512 (A5022)	MAC: 512 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA3-224 (A5022)	MAC: 224 Key Length: 32,160,1176	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA3-256 (A5022)	MAC: 256 Key Length: 32,160,1176	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA3-384 (A5022)	MAC: 384 Key Length: 32,160,1176	KAT	CAST	Log message,	Sign	Power On,

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Module halt on failure		Request, Periodic
HMAC-SHA3-512 (A5022)	MAC: 512 Key Length: 32,160,1176	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
KAS-ECC-SSC Sp800-56Ar3 (A5022)	Curve: P-384 Scheme: ephemeralUnified KAS Role: Initiator, Responder	KAT	CAST	Log message, Module halt on failure	Initiator, Responder	Power On, Request, Periodic
KAS-IFC-SSC (A5022)	Scheme: KAS2 KAS Role: Initiator,Responder KeyGenerationMethod: rsakpg2-basic Modulo: 2048,4096 HashFunctionZ: SHA2-512	KAT	CAST	Log message, Module halt on failure	Initiator, Responder	Power On, Request, Periodic
KDA TwoStep SP800-56Cr2 (A5022)	L: 2048 SaltLen: 128, FixedInfoPattern: "label||algorithmId||uPartyInfo||vPartyInfo" FixedInfoEncoding: Concatenation KDF Mode: Counter MAC: CMAC-AES128 CounterLoc: "before fixed data" CounterLen: 32, IV Len: 0 zLength: 496, 2192	KAT	CAST	Log message, Module halt on failure	KDA	Power On, Request, Periodic
KDF SP800-108 (A5022)	RF: CMAC_AES128 CounterLoc: Before Fixed Data CounterLen: 32 COUNT=0 FixedInputLen: 72 L: 360,1024	KAT	CAST	Log message, Module halt on failure	KBKDF	Power On, Request, Periodic
KTS-IFC (A5022)	Scheme: KTS-OAEP-basic KAS Role: Responder KeyGenMethod: rsakpg1-basic Modulo: 4096 FixedPubExp: 010001 L: 512 Hash: SHA2-512	KAT	CAST	Log message, Module	Responder	Power On, Request

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				halt on failure		, Periodic
LMS KeyGen (A5022)	LMS Mode: LMS_SHA256_M24_H5, LMS_SHA256_M32_H5 LMOTS Mode: LMOTS_SHA256_N24_W4, LMOTS_SHA256_N32_W8	KAT	CAST	Log message, Module halt on failure	KeyGen	Power On, Request, Periodic
LMS SigGen (A5022)	LMS Mode: LMS_SHA256_M24_H5, LMS_SHA256_M32_H5 LMOTS Mode: LMOTS_SHA256_N24_W2, LMOTS_SHA256_N32_W1	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
LMS SigVer (A5022)	LMS Mode: LMS_SHA256_M24_H15,LMS_SHA256_M24_H10,LMS_SHA256_M24_H20,LMS_SHA256_M24_H5,LMS_SHA256_M24_H25,LMS_SHA256_M32_H15,LMS_SHA256_M32_H25,LMS_SHA256_M32_H10,LMS_SHA256_M32_H20,LMS_SHA256_M32_H5 LMOTS Mode: LMOTS_SHA256_N24_W8,LMOTS_SHA256_N24_W1,LMOTS_SHA256_N24_W2,LMOTS_SHA256_N24_W4,LMOTS_SHA256_N32_W8,LMOTS_SHA256_N32_W1,LMOTS_SHA256_N32_W2,LMOTS_SHA256_N32_W4	KAT	CAST	Log message, Module halt on failure	Verify	Power On, Request, Periodic
PBKDF (A5022)	HMAC Algs: SHA-1,SHA2-224,SHA2-256,SHA2-384,SHA2-512 Key Lengths: 1792,800,1392,272,1744 Iteration Count: 764,26,408,10,437	KAT	CAST	Log message, Module halt on failure	PBKDF	Power On, Request, Periodic
RSA SigGen (FIPS186-5) (A5022)	Modulo: 2048 Hash: SHA2 256	KAT	CAST	Log message, Module	Sign	Power On, Request

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				halt on failure		, Periodic
RSA SigVer (FIPS186-5) (A5022)	Modulo: 2048 Hash: SHA2 256	KAT	CAST	Log message, Module halt on failure	Verify	Power On, Request, Periodic
SHA-1 (A5022)	Msg Len: 640 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-224 (A5022)	Msg Len: 448 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-256 (A5022)	Msg Len: 448 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-384 (A5022)	Msg Len: 896 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA2-512 (A5022)	Msg Len: 896 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA3-224 (A5022)	Msg Len: 0, 56 bits	KAT	CAST	Log message,	Hash	Power On,

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Module halt on failure		Request, Periodic
SHA3-256 (A5022)	Msg Len: 0, 96 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA3-384 (A5022)	Msg Len: 0, 104 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
SHA3-512 (A5022)	Msg Len: 0, 152 bits	KAT	CAST	Log message, Module halt on failure	Hash	Power On, Request, Periodic
TDES-CBC (A5022)	Keying Option: 2 Key Length: 192	KAT	CAST	Log message, Module halt on failure	Decrypt	Power On, Request, Periodic
HMAC-SHA-1 (A5022)	MAC: 160 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic
HMAC-SHA-1 (A5021)	MAC: 160 Key Length: 256	KAT	CAST	Log message, Module halt on failure	Sign	Power On, Request, Periodic

Table 24: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
EDC (160 bits)	KAT	SW/FW Integrity	Power-on	Manual
EDC (256 bits)	KAT	SW/FW Integrity	Power-on	Manual

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ESV (Entropy Certificate #E97)	CRNGT	CAST	On Entropy Generation	Manual
RSA KeyGen (FIPS186-5) (A5022)	PCT	PCT	On RSA Keypair Generation	Manual
ECDSA KeyGen (FIPS186-5) (A5022)	PCT	PCT	On ECDSA Key Generation	Manual
Firmware Load Test	Signature Verification	SW/FW Load	On Firmware Update Service	Manual
AES-CBC (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CFB128 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CFB8 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CMAC (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CTR (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-ECB (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-OFB (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
DSA SigVer (FIPS186-4) (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
ECDSA SigGen (FIPS186-5) (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
ECDSA SigVer (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA2-224 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA2-256 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA2-384 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA2-512 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-224 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-256 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-384 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-512 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KAS-ECC-SSC Sp800-56Ar3 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-IFC-SSC (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KDA TwoStep SP800-56Cr2 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KDF SP800-108 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KTS-IFC (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
LMS KeyGen (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
LMS SigGen (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
LMS SigVer (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
PBKDF (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
RSA Decryption Primitive (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
RSA SigVer (FIPS186-4) (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA-1 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA2-224 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA2-384 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA2-512 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA3-224 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA3-256 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA3-384 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA3-512 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
TDES-CBC (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CBC (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CFB128 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CFB8 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-CMAC (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-ECB (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-GCM (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-GMAC (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-KW (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-KWP (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-OFB (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
AES-XTS Testing Revision 2.0 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
DSA SigVer (FIPS186-4) (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
ECDSA SigVer (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
Hash DRBG (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA2-224 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA2-384 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA2-512 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-224 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-256 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-384 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA3-512 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KAS-ECC-SSC Sp800-56Ar3 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KAS-IFC-SSC (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KDA TwoStep SP800-56Cr2 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KDF SP800-108 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
KTS-IFC (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
LMS KeyGen (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
LMS SigGen (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
LMS SigVer (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
PBKDF (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
RSA SigGen (FIPS186-5) (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
RSA SigVer (FIPS186-5) (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA-1 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA2-224 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA2-256 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA2-384 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA2-512 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA3-224 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-256 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA3-384 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
SHA3-512 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
TDES-CBC (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA-1 (A5022)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic
HMAC-SHA-1 (A5021)	KAT	CAST	Power-on, On Demand, CAST Timer (1hr min, 24hr default)	Manual and Automatic

Table 26: Conditional Periodic Information

As shown in the tables above, the module performs self-tests for the certified algorithms at Power-On and on a periodic basis to ensure FIPS 140-3 compliance.

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 CAST timer expires, the ICD command interface is shut down and all command processing stops while the full suite of Power-On Cryptographic Algorithm tests is run on all cryptographic libraries.

The CAST test result is written to the UHD (USB HSM Device) driver log for the M7 module. If the CAST test fails, the module will halt operation and stop processing commands until the next power cycle. On success, that CAST result is logged as well, and the module will re-enable its ICD command interface over the USB Target port and resume normal operation.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Service Error	Error on a function call that does not impact ability to operate securely	Service Execution Error	Automatic	Error status returned in command response
Fatal Error	Error of severity that requires the module to halt operation	On Demand (Service Execution) Service induced Fatal Errors occur on: Self-test failure Critical component (NVRAM, Flash, RTC) I/O failure USB communications failure RNG statistical test failure	Power cycle	Fatal Error status on display, Fatal Error message logged and sent to host, module operation halted

Table 27: Error States

On the failure of a Self-Test, the module will store a log of the failed test, display a fatal error status on the display, send a fatal log message to the host, and halt all operations. The only recovery from the Self-Test failure module halt 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.

A second method would be to alter the CAST timing interval for the Periodic Tests as outlined in Section 10.3.

A third method would be for the operator to initiate the Request HSM Self-Test service by issuing the corresponding command across the ICD command interface. That would also execute all of the Periodic Tests listed in Section 10.2.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Installation

The Luna M7 Cryptographic Module shall be inspected for tamper upon receipt as indicated in Section 7.1 above. The Module should be deployed in a secure environment that will protect the module from sophisticated attackers with direct access.

This is standard practice for high-value assets such as HSMs and forms part of a defense-in-depth approach to security.

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
- CCTV monitoring of areas containing the HSM to allow detection of activity in proximity to the HSM.

11.1.2 Initialization

Before using the module it must be initialized, after which it should be immediately configured into its Approved mode of operation. Prior to secure initialization of the module, access control relies on procedural controls only and the module should be received in the zeroized state with no initialized roles.

Note: The module shall be received in a zeroized state. To check the status of the module, use the ‘hsm showinfo’ LunaCM command. The front panel will also display ‘Zeroized’ when the module is in the zeroized state.

Initialization creates the HSM SO role, names the module, defines the authentication mode and associates the admin partition with a key cloning domain.

Initialization is performed using the ‘hsm init’ command from LunaCM or LunaSH.

It should be noted that the ‘hsm init’ command should only be run by the individual identified as the HSM Security Officer (SO).

Following initialization of the module, it should immediately be configured into its Approved mode of operation ahead of initialization of any further roles or creation of any stored key objects. Guidance on configuring the Approved mode of operation is provided in Section 2.4.

11.2 Administrator Guidance

As noted above, the Administrator should assume the HSM SO role and perform the module Initialization, setting the module into its Approved mode of operation and defining whether Password or PED based authentication will be used.

Refer to the Thales TCT T-series HSM documentation for further Administrator Guidance on performing tasks related to the Crypto Officer Role such as creating User partitions.

11.3 Non-Administrator Guidance

Refer to the Thales TCT T-series HSM documentation for further Non-Administrator Guidance on performing tasks related to the User Role such as performing cryptographic operations.

Further documentation on Administrator and Non-Administrator operations that can be performed on the cryptographic module in the T-Series Luna Backup HSM and Luna USB HSM products can be obtained on the Thales TCT Customer Portal at https://support.thalestct.com .

These documents include:

- Installation Guide
- Configuration Guide
- Appliance Administration Guide
- HSM Administration Guide
- LunaCM Command Reference Guide
- LunaSH Command Reference Guide
- SDK Reference Guide
- Utilities Reference Guide

11.4 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.

12 Mitigation of Other Attacks

N/A for this module.