Thales Luna K7 Cryptographic Module

NON-PROPRIETARY SECURITY POLICY

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

FIPS 140-2, Level 3

Document Information

Document Part Number	002-010935-001
Release Date	18th May 2020

Revision History

Revision	Date	Reason
U	18th May 2020	Updated picture of Thales Luna Network HSM.
T	18th May 2020	Updated picture of Thales Luna PIN Entry Device.
R	15th May 2020	Rebranded document to Thales including updating product name throughout. Added Bootloader version 1.1.4.

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

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

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

> This document shall not be posted on any network computer or broadcast in any media other than by on the NIST CMVP Validation List and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

ACRONYMS

Acronyms and abbreviations

Term	Definition
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CU	Crypto User
DAK	Device Authentication Key
DAC	Device Authentication Certificate
DH	Diffie Hellman
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
FIPS	Federal Information Processing Standard
GSK	Global Storage Key
HOC	Hardware Origin Certificate
HOK	Hardware Origin Key
HSE-BBRAM	High-speed erase battery backed RAM
HSM	Hardware Security Module
KAT	Known Answer Test
ICD	Interface Control Design/Document
KDF	Key Derivation Function
KEK	Key Encryption Key
MAC	Message Authentication Code

Term	Definition
Masking	A Thales term to describe the encryption of a key for use only within a Thales cryptographic module.
MIC	Manufacturer’s Integrity Certificate
MIK	Manufacturer’s Integrity Key
PSK	Partition Storage Key
PCI-E	Peripheral Component Interconnect
PEC	Password Encryption Certificate
PED	PIN Entry Device
PEK	Password Encryption Key
PKCS	Public-Key Cryptography Standards
RNG	Random Number Generator
RPK	Remote PED Key
RPV	Remote PED Vector
SADK	Secure Audit Domain Key
SALK	Secure Audit Logging Key
SMK	Security Officer’s Master Key
SO	Security Officer
STC	Secure Trusted Channel
STM	Secure Transport Mode
TUK	Token or Module Unwrapping Key
TVK	Token or Module Variable Key
TWC	Token or Module Wrapping Certificate
USK	User’s Storage Key

PREFACE

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

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

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

> product manuals and technical support literature can be found through the customer support portal at: https://supportportal.thalesgroup.com/csm

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

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

1 Introduction

1.1 Purpose

This non-proprietary document describes the security policies enforced by Thales Luna K7 Cryptographic Module and Thales Luna K7 Cryptographic Module for Thales Luna Network HSM.

1.2 Scope

This document applies to Hardware Versions 808-000048-002, 808-000066-001 or 808-000073-001 with Firmware Versions 7.0.1, 7.0.2, 7.0.3 or 7.3.3, with Boot Loader Versions 1.1.1, 1.1.2 or 1.1.4

The security policies described in this document apply to the Thales Luna K7 Cryptographic Module only and do not include any security policy that may be enforced by the host appliance or server.

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

- A standalone device called the Thales Luna PCIe HSM; or
- An embedded device in the Thales Luna Network HSM.

The security policies described in this document apply to the PED and Password Authentication (FIPS Level 3) configurations of the Thales Luna K7 Cryptographic Module only and do not include any security policy that may be enforced by the host appliance or server.

The module is supplied configured for either Password or PED based authentication from a loaded license file.

1.3 Validation Overview

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

Table 1: FIPS 140-2 Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles and Services and Authentication	3
Finite State Machine Model	3
Physical Security	3 + EFP
Operational Environment	N/A
Cryptographic Key Management	3

Security Requirements Section	Level
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3
Cryptographic Module Security Policy	3

1.4 Functional Overview

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

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

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

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

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

2 Module Overview

2.1 Module Specification

The cryptographic module is a multi-chip embedded hardware module which is available by itself as a Thales Luna K7 Cryptographic Module or embedded within the Thales Luna Network HSM.

The cryptographic boundary[1] of the module is shown in Figure 2-1. The cryptographic boundary is defined as the metal enclosure on the top and bottom sides of the PCI-E card as outlined. The fans depicted alongside the removable backup battery are not included in the cryptographic boundary.

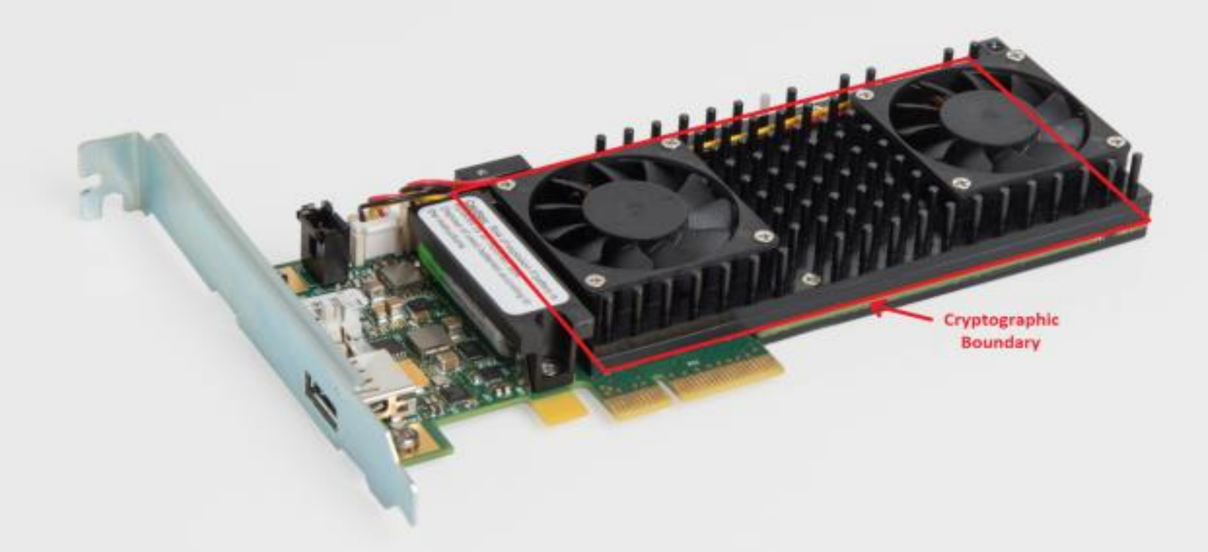

Figure 2-1: Thales Luna K7 Cryptographic Module cryptographic boundary

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

Figure 2-2: Thales Luna Network HSM

2.2 Ports and Interfaces

The module supports the following physical ports and interfaces:

- PCI-E interface
- USB port
- Serial port
- Power supply
- Battery
- LED
- External event input
- Decommission input

Table 2-1: Mapping of FIPS 140-2 Interfaces to Physical and Logical Interfaces

FIPS 140-2 Interface	Physical Interface	Logical Interface
Data Input	PCI-E interface	Data I/O Luna ICD Logical Trusted Path (Remote PED) Bootloader command protocol
	USB	Physical Trusted Path (Local PED)
	Serial interface	Bootloader command protocol
Data Output	PCI-E interface	Data I/O Luna ICD Logical Trusted Path (Remote PED) Bootloader command protocol

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

2.2.1 Trusted Path

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

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

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

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

> Blue (Security Officer) PED Key – for the storage of HSM Security Officer, Partition Security Officer and Administrator authentication data[2];

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

- Black (Crypto Officer) PED Key – for the storage of Crypto Officer authentication data;
- Grey (Crypto User) PED Key – for the storage of Crypto User authentication data;
- Red (Cloning Domain) PED Key – for the storage of the cloning domain data, used to control the ability to clone to another cryptographic module or to a backup module; and
- White (Audit Officer) PED Key – for the storage of Audit Officer authentication data.

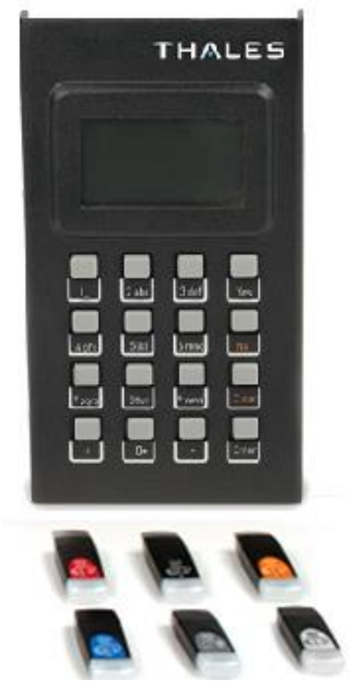

Figure 2-3: Thales Luna PIN Entry Device and iKey

2.2.2 Remote PED

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

The logical path between the module and the Remote Luna PED is secured in the manner described below.

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

To establish the secure connection, the RPK must be inserted into the Luna PED connected to a management workstation. The Luna PED extracts the RPV, and the Luna PED and the cryptographic module then participate in an ephemeral Diffie-Hellman key agreement session. The derived shared secret is then XORed with the RPV to produce the key to be used for the session. An exchange of encrypted random nonces is performed to authenticate both ends of the transmission. All traffic between the PED and the cryptographic module is encrypted using AES 256 OFB.

2.2.3 Secure Messaging

Each partition can individually be configured to use a secure messaging feature called Secure Trusted Channel (STC). An STC channel is a cryptographic tunnel established between a partition and a host/client application. The STC channel is designed to provide both confidentiality and integrity on all ICD commands that are sent to the partition.

STC for a partition can be configured by registering one or more host/client RSA public keys with a partition. Once configured, the partition will reject any ICD commands[3] that are not delivered to the module through an STC channel.

An STC channel is established by using the partition STC public key and a registered client RSA key to exchange ephemeral DH public keys (SP800-56B Key Transport), which are in turn used to derive (SP800-56A key agreement) tunnel encryption, decryption and HMAC keys.

2.3 Roles and Services

2.3.1 Roles

The Thales Luna K7 Cryptographic Module supports the following authenticated roles:

> HSM Security Officer (HSM SO)

- Module-level role
- Initializes and configures the module for operation
- Creates user partitions
- Performs key management tasks for the admin partition
- Performs cryptographic operations for the admin partition
- Manages Administrator role[4]

> Administrator

- Optional admin partition-level Crypto Officer like role
- Performs key management tasks for the admin partition
- Performs cryptographic operations for the admin partition

> Audit Officer (AO)

- Module-level role
- Initializes, configures, and manages secure audit logging

> Partition Security Officer (PSO)

- User partition-level role
- Configures the partition policy settings and performs security administration tasks within the user partition

[3] Status commands and commands required to setup an STC channel are allowed to pass outside of the STC tunnel.

  - Manages Crypto Officer role[4]
- Crypto Officer (CO)
  - User partition-level role
  - Performs key management tasks for the user partition
  - Performs cryptographic operations for the user partition
  - Manages Crypto User role[4]
- Crypto User (CU)
  - Optional user partition-level read-only role
  - Performs cryptographic operations for the user partition

The module also supports the following unauthenticated role:

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

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

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

FIPS 140-2 Role	Thales Luna K7 Role	Role Scope
Crypto Officer	HSM Security Officer	Module
	Audit Officer	Module
	Partition Security Officer	User Partition
User	Administrator	Admin Partition
	Crypto Officer	User Partition
	Crypto User	User Partition
Unauthenticated User	Public User	Module/Partition

2.3.2 Services

All services listed in Table 2-3 can be accessed in FIPS 140-2 Approved mode and non-Approved mode. The services listed in Table 2-3 use the security functions listed in Table 2-6, Table 2-7, and section 2.6.2. When the module is operating in FIPS 140-2 Approved mode as described in Section 3.1, the non-Approved Security Functions in section 2.6.2 are disabled and cannot be used for these services. The non-Approved functions in section 2.6.2 can only be accessed through the services when the module is in non-Approved mode.

[4] Role is responsible for managing another role using the services (Initialize Role, Reset Role Authentication Data) as defined in Table 2-3

Table 2-3 Roles and Access Rights by Service

Service	Cryptographic Keys and CSPs	Type(s) of Access	Role						
			HSM Security Officer	Partition Security Officer	Crypto Officer	Crypto User	Public User	Audit Officer	Administrator
Show Status	N/A	N/A	x	x	x	x	x	x	x
Self-test	N/A	N/A	x	x	x	x	x	x	x
Initialize Module	DRBG State	Use	x						
	Authentication data, SMK, PSK, KCV	Write							
Configure Module Policy[5]	N/A	N/A	x						
Create Partition	N/A	N/A	x						
Initialize Partition	DRBG State	Use		x					
	Authentication data, USK, PSK, KCV	Write							
Configure Partition Policy[5]	N/A	N/A		x					
Initialize Role	Authentication Data, USK, PSK	Write	x	x	x				
Login	Authentication data, USK, PSK	Use					x		
Logout	N/A	N/A	x	x	x	x		x	x
Reset Role Authentication Data	Authentication Data, USK, PSK	Write	x	x	x				
Change Role Authentication Data	Authentication Data, USK, PSK	Use, Write	x	x	x	x		x	x
Zeroize Module	Authentication data, SMK, PSK, KCV, LKCV, SADK, symmetric keys, asymmetric key pairs	Erase	x	x	x	x	x	x	x
Zeroize Partition	Authentication data, USK, PSK, KCV, LKCV, symmetric keys, asymmetric key pairs	Erase	x	x	x	x	x	x	x

[5] May invoke Zeroize Module service

Service	Cryptographic Keys and CSPs	Type(s) of Access	Role						
			HSM Security Officer	Partition Security Officer	Crypto Officer	Crypto User	Public User	Audit Officer	Administrator
Delete Partition	Authentication data, USK, PSK, KCV, LKCV, symmetric keys, asymmetric key pairs	Erase	x						
Firmware Update	GSK, Root Certificate	Use Write (firmware only)	x						
Configuration Update	Root Certificate	Use	x						
	Authentication data, USK, PSK, KCV, LKCV, symmetric keys, asymmetric key pairs	Erase (may invoke Zeroize Module and Zeroize Partition)							
Generate Random Data	DRBG State	Use	x	x	x	x		x	x
Key Generation	DRBG State	Use	x		x				x
	Symmetric keys	Write							
Key Pair Generation	DRBG State	Use	x		x				x
	Asymmetric key pairs	Write							
Domain Parameter Generation	DRBG State	Use	x		x				x
	Domain Parameters	Write							
Wrap Symmetric Key	KTS symmetric/asymmetric wrapping key	Use (wrapping key) Write (unwrapped key)	x		x				x
Unwrap Symmetric Key	symmetric key, symmetric/asymmetric unwrapping key	Use (wrapping key) Write (unwrapped key)	x		x				x
Unwrap Asymmetric Key	asymmetric key, symmetric unwrapping key	Use (wrapping key) Write (unwrapped key)	x		x				x

Service	Cryptographic Keys and CSPs	Type(s) of Access	Role						
			HSM Security Officer	Partition Security Officer	Crypto Officer	Crypto User	Public User	Audit Officer	Administrator
Key Unmask	KCV	Use	x		x				x
	symmetric key, asymmetric key	Write							
Key Agreement	asymmetric key, symmetric key	Use Write	x		x				x
Key Derivation	symmetric key	Use, Write	x		x				x
HASH	N/A	N/A	x		x	x			x
Partition Backup / Restore	Asymmetric private keys, Symmetric keys	Transfer[6]	x		x				
	DRBG State, ROOT, MIC, HOC, TWC, TUK, KCV	Use							
Symmetric Encrypt/Decrypt	DRBG State, Symmetric keys	Use	x		x	x			x
Asymmetric Signature	DRBG State, RSA, DSA, ECDSA, EDDSA private keys	Use	x		X	X			x
Asymmetric Verification	RSA, DSA, ECDSA, EDDSA public keys	Use	x		x	x			x
Store Data Object	Non-cryptographic data	Write	x		x	x	x		x
Read Data Object	Non-cryptographic data	Read	x		x	x	x		x

[6] Transfer means moving a key using the cloning protocol from one cryptographic module to another.

Service	Cryptographic Keys and CSPs	Type(s) of Access	Role						
			HSM Security Officer	Partition Security Officer	Crypto Officer	Crypto User	Public User	Audit Officer	Administrator
Initialize Secure Audit Logging	DRBG State	Use						x	
	Authentication Data, SADK	Write							
Change Audit Officer's Password	DRBG State	Use						x	
	Authentication data	Read, Write							
Configure Secure Audit Logging	N/A	Read, Write						x	
Synchronize Module's clock with the Host system's clock	N/A	Write						x	
Verify, Import, and Export secure audit log files	SALK	Use						x	
Show secure audit log status	N/A	Read						x	
Import and Export the Wrapped Secure Audit Logging Key	SALK	Write, Read						x	

2.3.3 Authentication

All roles except for the Public User must authenticate to the module by providing their authentication data. Table 2-3 and Table 2-4 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. Optionally, the Crypto-Officer and Crypto-User roles can be configured to use two-factor authentication by also assigning a password to the role.

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

Regardless of configuration (PED or Password), the password is delivered to the module encrypted with the module's Password Encryption Key (PEC) using RSA-OAEP and a random nonce to prevent replay attacks.

Table 2-3 Roles and Required Identification and Authentication

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

Table 2-4 Strengths of Authentication Mechanisms

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

2.3.4 Activation

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

Once activated, a role stays activated until the role is explicitly deactivated, deleted or the module is reset[7].

2.3.5 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.

[7] A module is reset in response to an External Event, Decommission signal and EFP violations, loss of power and a request from a host application.

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

2.4 Physical Security

The Luna cryptographic module is a multi-chip embedded module as defined by FIPS PUB 140-2 section 4.5. The module is enclosed in a strong metal enclosure that provides tamper-evidence. Any tampering that might compromise a module's security is detectable by visual inspection of the physical integrity of a module. The HSM Security Officer should perform a visual inspection of the module at regular intervals. Within the metal enclosure, a hard opaque epoxy covers the circuitry of the cryptographic module. Attempts to remove this epoxy will cause sufficient damage to the cryptographic module so that it is rendered inoperable.

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

2.4.1 External Event

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

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

2.4.2 PCI-E Card Removal

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

2.4.3 Environmental Failure Protection

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

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

Note, under-voltage conditions cannot be reliably distinguished from a power cycle.

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

2.4.4 Decommission

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

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

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

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

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

2.4.5 Secure Transport Mode

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

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

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

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

2.4.6 Fault Tolerance

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

A module shall maintain its secure state[8] in the event of data input / output failures. When data input / output capability is restored the module will resume operation in the state it was prior to the input / output failure.

2.5 Operational Environment

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

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

2.6 Cryptographic Key Management

2.6.1 FIPS-Approved Algorithm Implementations

The FIPS-Approved algorithms implemented by the module can be found in Table 2-6.

Table 2-6 FIPS-Approved Algorithm Implementations

Approved Security Functions	Certificate No.
Symmetric Encryption/Decryption	
AES: ECB, CBC, OFB, CTR, CFB8, CFB128, GCM, XTS, KW, KWP	#4753
AES: GCM[9]	#4754
Triple-DES (3-key): ECB, CBC, OFB, CTR, CFB8, CFB64	#2525
Hashing	
SHA: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	#3896
SHA[10]: SHA-256, SHA-512 (Byte Only)	#3897
SHA: SHA-1, SHA-384 (Byte Only)	#3951 and #3952
Message Authentication Code	
HMAC: HMAC-SHA-1[11], HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	#3166
Triple-DES: MAC (based on Certificate No. #2525) (Vendor Affirmed) CMAC	#2525
AES: CMAC	#4753
Asymmetric	
RSA:	#2597

[9] The module generates IVs internally using the Approved DRBG which are at least 96-bits in length.

[10] Alternate implementation that is used under certain configurations.

[11] Only keys of 112 bits or greater are allowed in FIPS mode when using HMAC-SHA-1.

Approved Security Functions	Certificate No.
Key Generation, Signature Generation, Signature Verification	
RSA[10]: Key Generation	#2598
RSA: Signature Verification, Signature Generation	#2631 and #2632
DSA: Parameter Generation, Key Generation, Signature Generation, Signature Verification	#1274
DSA[10]: Parameter Generation, Key Generation	#1275
ECDSA: Key Generation, Signature Generation, Signature Verification Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	#1188
ECDSA[10]: Key Generation Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	#1189
ECDSA (CVL): Signature Generation Component Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	#1392
RSA (CVL): Decryption Primitive	#1431
Key Agreement Scheme	
ECC: Ephemeral Unified, OnePassDH FCC: dhHybrid1, dhEphem, dhHbryidOneFlow, dhOneFlow	#133
FCC[10]: dhHybrid1, dhEphem, dhHbryidOneFlow, dhOneFlow	#134
Key Transport	
KTS (AES Cert. #4753)	#4753
Key Derivation Function	
Key-Based Key Derivation Function (KBKDF): Counter Mode	#152

Approved Security Functions	Certificate No.
Random Number Generation	
NIST SP 800-90A DRBG (CTR) AES 256	#1634

Table 2-7 Allowed Security Function for the Firmware Implementation

Allowed Security Functions
Key Agreement
Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
Key Transport
RSA (key wrapping; key establishment methodology provides between 112 and 152 bits of encryption strength) (based on Certificate No. #2597)
RSA (key wrapping; key establishment methodology provides between 112 and 152 bits of encryption strength) (based on Certificate No. #2598)[10]
AES (key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength) (based on Certificate No. #4753)
Triple-DES (key unwrapping; key establishment methodology provides 112 bits of encryption strength) (based on Certificate No. #2525)
Entropy Source (non-FIPS Approved but Allowed)
Hardware Random Number Generator (free-running local oscillators)

2.6.2 Non-Approved Security Functions

The following Non-FIPS Approved security functions are implemented on the cryptographic module but not available for use when the module has been configured to operate in FIPS-approved mode (see section 3.1 for guidance on configuring FIPS-approved mode):

> **Symmetric Encryption/Decryption**

- DES
- RC2
- RC4
- RC5
- CAST3
- CAST5

  - SEED
  - ARIA
- **Hashing**
  - MD2
  - HAS-160
  - SM3
- **Message Authentication Code**
  - AES MAC (non-compliant)
  - DES-MAC
  - RC2-MAC
  - RC5-MAC
  - CAST3-MAC
  - CAST5-MAC
  - SEED-MAC
  - ARIA-MAC
  - SSL3-MD5-MAC
  - SSL3-SHA1-MAC
  - HMAC (Cert #3166 – non-compliant less than 112 bits of encryption strength)
- **Asymmetric**
  - KCDSA
  - RSA X.509
  - RSA (Cert #2597, Cert #2598 – non compliant less than 112 bits of encryption strength)
  - DSA (Cert #1274, Cert #1275 – non-compliant less than 112 bits of encryption strength)
  - ECDSA (Cert #1188, Cert #1189 – non-compliant less than 112 bits of encryption strength)
  - EDDSA
- **Generate Key**
  - DES
  - RC2
  - RC4
  - RC5
  - CAST3
  - CAST5

- SEED
- ARIA
- GENERIC-SECRET
- SSL PRE-MASTER
- BIP32

> **Key Agreement**

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

> **Key Transport**

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

2.7 Critical Security Parameters

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

Table 2-7 Keys and Critical Security Parameters Used in the Module

Keys and CSPS	CSP Type	Generation	Input / Output	Storage	Destruction	Description
User Password (if PED configuration and Optionally selected)	7 - 64 character data string	N/A	Input from host using ICD communication path	Flash memory encrypted with PSK	N/A	User provided password input by the operator as a second factor of authentication data.
PED Authentication Data (if PED configuration)	48-byte random value	AES-CTR DRBG	Input / Output via direct connection to PED	Not stored On module	N/A	A 48-byte random value that is generated by the module when a role is created and is written out to the PED key via the Trusted Path.
Password (Authentication Data if Password configuration)	7 - 255 character data string	N/A	Input from host using ICD communication path	Not stored On module	N/A	User provided password input by the operator as authentication data.
Key Cloning Domain Vector (KCV)	48-byte random value	AES-CTR DRBG	Input/Output via direct connection to PED	Flash Memory encrypted with PSK	N/A	48-byte value that is used to control a partition's ability to participate in the cloning protocol. It is either generated by the module or imprinted onto the module at the time the module is initialized. The value is output from the original module in the domain onto a PED key to enable initializing additional modules into the same domain.
User Storage Key (USK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with User's Authentication Data and KEK	N/A	This key is used to encrypt all sensitive attributes of all private objects owned by the User.
Security Officer Master Key (SMK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with SO's Authentication Data and KEK	N/A	This key is used to encrypt all sensitive attributes of all private objects owned by the SO.
Partition Storage Key (PSK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with USK	N/A	This key is unique per-partition and used to encrypt all CSP that are shared by all roles of a given partition.
Global Storage Key (GSK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with PSK	N/A	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.
Root Certificate	RSA-4096 public key certificate	Loaded at manufacturing	Certificate Output in Plaintext	Flash memory in plaintext	N/A	The X.509 public key certificate corresponding to the Root Key. It is self-signed. Used in verifying Manufacturing Integrity Certificate (MIC) and firmware updates.
Manufacturer's Integrity Certificate (MIC)	RSA-4096 public key certificate	Loaded at manufacturing	Certificate Output in Plaintext	Flash memory in plaintext	N/A	The X.509 public key certificate corresponding to the Manufacturing Integrity Key (MIK). It is signed by the Root Key. Used in verifying

Keys and CSPS	CSP Type	Generation	Input / Output	Storage	Destruction	Description
						Hardware Origin Certificates (HOCs), which are generated in response to a customer function call to provide proof of hardware origin.
Hardware Origin Key (HOK)	RSA 4096 bit private key	FIPS 186-4	Not Input or Output	Flash memory encrypted with GSK	N/A	A 4096 bit RSA private key used to sign certificates for other device key pairs, such as the TWC. It is generated at the time the device is manufactured.
Hardware Origin Certificate (HOC)	RSA-4096 public key certificate	Loaded at manufacturing	Certificate Output in Plaintext	Flash memory in plaintext	N/A	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.
Password Encryption Key (PEK)	RSA 4096 bit private key	FIPS 186-4	Not Input or Output	Working RAM in plaintext	N/A	A 4096 bit RSA private key used to decrypt user passwords that are provided to the module. It is generated the first time it is required.
Password Encryption Certificate (PEC)	RSA-4096 public key certificate	FIPS 186-4	Certificate Output in Plaintext	Working RAM in plaintext	N/A	The X.509 public key certificate corresponding to the PEK. It is created and signed by the HOK the first it is required.
Token or Module Unwrapping Key (TUK)	RSA-2048 bit private key	FIPS 186-4	Not Input or Output	Flash memory encrypted with GSK	N/A	A 2048-bit RSA private key used in the cloning protocol.
Token or Module Wrapping Certificate (TWC)	RSA-2048 public key certificate	FIPS 186-4	Certificate Output in Plaintext	Flash memory plaintext	N/A	The X.509 public key certificate corresponding to the TUK. It is signed by the HOK. Used in exchange of session encryption key as part of the handshake during the cloning protocol.
Device Authentication Key (DAK)	RSA 2048 bit private key	FIPS 186-4	Not Input or Output	Flash memory encrypted with GSK	N/A	2048-bit RSA private key used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
Device Authentication Key (DAC)	RSA-2048 public key certificate	FIPS 186-4	Certificate Output in Plaintext	Working RAM in plaintext	N/A	The X.509 public key certificate corresponding to the DAK. It is signed by the HOK. Used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
ECC Manufacturing Integrity Certificate (ECC MIC)	ECC P-384 public certificate	Loaded at manufacturing	Certificate Output in Plaintext	Flash memory plaintext	N/A	The X.509 public key certificate corresponding to the ECC Manufacturing Integrity Key (ECC MIK). It is self-signed.
ECC Hardware Origin Key (ECC HOK)	ECC P-384 private key	FIPS 186-4	Not Input or Output	Flash memory encrypted with GSK	N/A	ECC P-384 private key used to sign other device keys and used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.
ECC Hardware Origin Certificate (ECC HOC)	ECC P-384 public certificate	FIPS 186-4	Certificate Output in Plaintext	Flash memory plaintext	N/A	The X.509 public key certificate corresponding to the ECC HOK. It is signed by the ECC Manufacturing Integrity Key (ECC MIK). It is used for a specific PKI implementation requiring assurance that a key or a specific action originated within the hardware crypto module.

Keys and CSPS	CSP Type	Generation	Input / Output	Storage	Destruction	Description
ECC Device Authentication Key (ECC DAK)	ECC P-384 private key	FIPS 186-4	Not Input or Output	Flash memory encrypted with GSK	N/A	ECC P-384 private key.
ECC Device Authentication Certificate (ECC DAC)	ECC P-384 public certificate	Loaded at manufacturing	Certificate Output in Plaintext	Flash memory plaintext	N/A	The X.509 public key certificate corresponding to the ECC DAK. It is signed by the ECC HOK.
Token or Module Variable Key (TVK) (if PED configuration)	AES-256	AES-CTR DRBG	Not Input or Output	HSE-BBRAM in plaintext	Zeroized in response to physical security measures	It is used to encrypt authentication data stored for auto-activation purposes.

Keys and CSPS	CSP Type	Generation	Input / Output	Storage	Destruction	Description
Key Encryption Key (KEK)	AES-256	AES-CTR DRBG	Not Input or Output	HSE-BBRAM in plaintext	Zeroized in response to physical security measures	The KEK encrypts all sensitive values and is zeroized in response to a decommission signal.
Remote PED Vector (RPV) (if PED configuration)	256-bit secret value	AES-CTR DRBG	Input / Output via direct connection to PED	Flash memory encrypted with GSK	Zeroized via ICD command	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.
DRBG Key	AES-256	Hardware Random Source	Not Input or Output	Working RAM in plaintext	Power Cycle	32 bytes AES key stored in the RAM. Used in an implementation of the NIST SP 800-90A CTR (AES) DRBG.
DRBG Seed	384 bits	Hardware Random Source	Not Input or Output	Working RAM in plaintext	Power Cycle	Random seed data drawn from the Hardware RBG and used to seed an implementation of the NIST SP 800-90A CTR (AES) DRBG.
DRBG V	128 bits	Hardware Random Source	Not Input or Output	Working RAM in plaintext	Power Cycle	Part of the secret state of the approved DRBG. The value is generated using the methods described in NIST SP 800-90A.
DRBG Entropy Input	384 bits	Hardware Random Source	Not Input or Output	Working RAM in plaintext	Power Cycle	The 384-bit entropy value used to initialize the approved DRBG.
Secure Audit Domain Key (SADK)	48-byte random value	AES-CTR DRBG	Input/Output via direct connection to PED	Flash Memory encrypted with USK	N/A	A 48-byte value, the first 32-bytes of which are used as an AES KW 256-bit key that is used to wrap/unwrap the SALK when it is exported / imported from / to the module. It is either generated by the module or imprinted onto the module at the time Audit role is initialized. The value is output from the original module onto a PED key to enable initializing the Audit role on additional modules into the same domain.
Secure Audit Logging Key (SALK)	256 bit HMAC key	AES-CTR DRBG	Input / Output encrypted	Flash memory in plaintext, Flash memory encrypted with SADK	N/A	A 256-bit key used to verify data integrity and authentication of the log messages. Saved in the parameter area of Flash memory.
Secure Transport Mode (STM) Nonce	992-bits	AES-CTR DRBG	Not Input or Output	HSE-BBRAM in plaintext	Zeroized in response to physical security measures	Random value used to create module fingerprint that is used to verify the module's integrity as part of the Secure Transport Mode feature.
Partition STC Private Key	2048-bit private key	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with GSK	Zeroized via ICD command	A 2048-bit RSA private key used in the STC protocol.
Partition STC Public Key	2048-bit public key	AES-CTR DRBG	Output in Plaintext	Flash memory in plaintext	Zeroized via ICD command	A 2048-bit RSA public key used in the STC protocol.
Partition STC Client/Host Public Keys	2048-bit public key	N/A	Public Key Input in Plaintext	Flash memory in plaintext	Zeroized via ICD command	A 2048-bit RSA public key used in the STC protocol.

2.7.1 Key Generation

Symmetric cryptographic keys are generated by the direct unmodified output of the module's NIST SP 800-90A DRBG. The DRBG output is also used as a seed for asymmetric key generation.

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

User passwords for authentication are generated by the operator.

2.7.2 Key Import and Export

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

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

The remaining keys and CSPs listed in Table 2 9 are not input to or output from the module.

Depending on the configuration of the module, the following methods of key entry and output may be available as a service (see section 2.3.2):

> **Key Cloning**

Key cloning uses a one-time AES key as a session key to encrypt an object being transferred from one Luna module to another. Objects transferred using the cloning protocol may be keys, user data, or module data. The AES session encrypting key is obtained by combining the 48 byte cloning domain value (randomly generated by the module) with random one-time data generated by source and target modules and exchanged using RSA 4096-based transport.

> **Key Wrap / Unwrap**

The key wrap operation encrypts a symmetric key value for output, using either an RSA public key or a symmetric key (KTS).

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

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

2.7.3 Key Storage

The module supports the following storage methods of keys and CSPs within the module:

> Stored in flash memory in plaintext

> Stored in flash memory encrypted with PED key and KEK if configured, otherwise authentication data and KEK

> Stored in flash memory encrypted with Global Storage Key

- Stored in flash memory encrypted with Partition Storage Key
- Stored in working RAM in plaintext
- Stored in tamperable HSE-BBRAM in plaintext.
- Stored in flash memory encrypted with User Storage Key
- Stored in flash memory encrypted with Security Officer Master Key
- Stored in flash memory in plaintext and encrypted with Audit role's User Storage Key
- Stored in flash memory encrypted with Secure Audit Domain Key

For a definition of how each key and CSP is stored, see Table 2-7.

2.7.4 Zeroization

The module supports the following zeroization techniques for plaintext keys and CSPs:

- Zeroized by power cycle of the module
- Zeroized via ICD command
- Zeroized in response to physical security measures
- Zeroized as part of a decommission signal
- Zeroized when moving to/from FIPS 140-2 Approved mode and non-Approved mode of operation
- Zeroized when the configured threshold for failed HSM Security Officer login attempts is reached
- Zeroized (partition) when the configured threshold for failed Partition Security Officer login attempts is reached

For a definition of how each key and CSP is zeroized, see Table 2-7.

2.7.5 Electromagnetic Interference/Electromagnetic Capability

The cryptographic module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

2.8 Self Tests

2.8.1 Power-On Self Tests

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

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

Table 2-8 Power-On Self-Tests – Module Integrity

Test	When Performed	Where Performed	Indicator
Boot loader performs an RSA 4096-bit SHA-384 signature verification of itself	Power-on	Firmware	Error output and module halt
Boot loader performs an RSA 4096-bit SHA-384 signature verification of the firmware prior to firmware start	Power-on/Request	Firmware	Error output and module halt

Table 2-9 Power-On Self-Tests – Cryptographic Implementations

Test	When Performed	Where Performed	Indicator
DRBG Instantiate Function Known Answer Test (KAT)	Power-on	Firmware	Error output and module halt[12]
DRBG Generate Function KAT	Power-on	Firmware	Error output and module halt[12]
DRBG Reseed Function KAT	Power-on	Firmware	Error output and module halt[12]
DRBG conditional tests	Power-on/Request	Firmware	Error output and module halt[12]
Triple-DES KATs	Power-on/Request	Firmware	Error output and module halt[12]
SHA-1 KAT	Power-on/Request	Firmware	Error output and module halt[12]
SHA-224 KAT	Power-on/Request	Firmware	Error output and module halt[12]
SHA-256 KAT	Power-on/Request	Firmware	Error output and module halt[12]
SHA-384 KAT	Power-on/Request	Firmware	Error output and module halt[12]
SHA-512 KAT	Power-on/Request	Firmware	Error output and module halt[12]
HMAC SHA-1 KAT	Power-on/Request	Firmware	Error output and module halt[12]
HMAC SHA-224 KAT	Power-on/Request	Firmware	Error output and module halt[12]
HMAC SHA-256 KAT	Power-on/Request	Firmware	Error output and module halt[12]
HMAC SHA-384 KAT	Power-on/Request	Firmware	Error output and module halt[12]

[12] Module halt only occurs for failures for power-on tests.

Test	When Performed	Where Performed	Indicator
HMAC SHA-512 KAT	Power-on/Request	Firmware	Error output and module halt[12]
RSA sig-gen KAT	Power-on/Request	Firmware	Error output and module halt[12]
RSA sig-ver KAT	Power-on/Request	Firmware	Error output and module halt[12]
DSA sig-gen KAT	Power-on/Request	Firmware	Error output and module halt[12]
DSA sig-ver KAT	Power-on/Request	Firmware	Error output and module halt[12]
Diffie-Hellman KAT	Power-on/Request	Firmware	Error output and module halt[12]
AES KATs	Power-on/Request	Firmware	Error output and module halt[12]
AES-GCM KAT	Power-on/Request	Firmware	Error output and module halt[12]
ECDH KAT	Power-on/Request	Firmware	Error output and module halt[12]
ECDSA sig-gen KAT	Power-on/Request	Firmware	Error output and module halt[12]
ECDSA sig-ver KAT	Power-on/Request	Firmware	Error output and module halt[12]
KDF KAT	Power-on/Request	Firmware	Error output and module halt[12]

2.8.2 Conditional Self Tests

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

Table 2-10 Conditional Self-Tests

Test	When Performed	Where Performed	Indicator
NDRNG conditional tests[13]	Continuous	Firmware	Error output and module halt[12]
RSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output
DSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output
ECDSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware	Error output

[13] CRNGT, as described in Section 4.9.2 of FIPS 140-2, is only performed for the NDRNG and is not performed for the DRBG as permitted by FIPS IG 9.8 for modules implementing an approved DRBG from NIST SP800-90A.

Test	When Performed	Where Performed	Indicator
Firmware load test (4096-bit RSA sig ver)	On firmware update load	Firmware	Error output – module will continue with existing firmware

2.8.3 Mitigation of Other Attacks

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

3 Guidance

3.1 FIPS 140-2 Approved Mode of Operation

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

- “Allow Non-FIPS Algorithms”

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

The HSM Security Officer can confirm that the cryptographic module is in FIPS 140-2 Approved mode by executing the “hsm showinfo” command in the administration tools provided with the module. If the module is in FIPS 140-2 Approved mode the following message will be displayed, “The HSM is in FIPS 140-2 approved operation mode”. If the module is not in FIPS 140-2 Approved mode the following message will be displayed, “The HSM is NOT in FIPS 140-2 approved operation mode”.

In accordance to NIST guidance, operators are responsible for insuring that a single Triple-DES key shall not be used to encrypt more than 2^16 64-bit data blocks.

3.2 Firmware Loading

The module performs a firmware load test on all incoming firmware images. The module only allows properly formatted and signed firmware to be loaded. Valid firmware images are digitally signed using the Thales Firmware signature key. RSA (4096 bits) PKCS #1 V1.5 with SHA-384 is used as the approved signature method.