THALES
Building a future we can all trust

Thales Luna USB Hardware Security Module

NON-PROPRIETARY SECURITY POLICY

Includes configurations Cloning [CL], Signing - No backup [SNB] and Key Export [CKE]

FIPS 140-2 Level 2

Document Information

Document Part Number	002-000269-001
Release Date	March 22, 2021

Revision History

Revision	Date	Reason
17	November 18, 2020	The document has been updated to be consistent in style to other Thales SPs including updates to both branding and product name.
B	January 20, 2021	Removed 186-2 Signature Generation and updated Tamper Label Picture.
C	March 22, 2021	Removed typographical error.

Trademarks, Copyrights, and Third-Party Software

Disclaimer

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

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

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

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

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

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

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

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or

consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

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

CONTENTS

ACRONYMS AND ABBREVIATIONS

Term	Definition
ANSI	American National Standards Institute
CA	Certification Authority
CKE	Key Export with RA
CL	Cloning (a capability configuration used to allow the secure transfer of key objects from one module to another for backup and restore and object replication purposes).
CLI	Command Line Interface
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem
CSP	Critical Security Parameter
CU	Crypto User
DAK	Device Authentication Key
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
HA	High Assurance
HOC	Hardware Origin Certificate
HOK	Hardware Origin Key
HRNG	Hardware Random Number Generator
HSM	Hardware Security Module

Term	Definition
KAT	Known Answer Test
KDF	Key Derivation Function
KEK	Key Encryption Key
MAC	Message Authentication Code
Masking	A Thales term to describe the encryption of a key for use only within a Thales Hardware Security Module.
MIC	Manufacturer's Integrity Certificate
MIK	Manufacturer's Integrity Key
MSK	Manufacturer's Signature Key
MTK	Master Tamper Key
MVK	Manufacturers Verification Key
PCI	Peripheral Component Interconnect
PED	PIN Entry Device
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PRNG	Pseudo-Random Number Generator
PSK	Partition Storage Key
PSO	Partition Security Officer
PSS	Probabilistic Signature Scheme
RA	Registration Authority
RNG	Random Number Generator
RPED	Remote PED
RPK	Remote PED Key
RPV	Remote PED Vector
SA	Server-Attached
SADK	Security Audit Domain Key

Term	Definition
SALK	Security Audit Logging Key
SCU	Secure Capability Update
SGSK	Secondary Global Storage Key
SFF	Small Form Factor
SHS	Secure Hash Standard
SMK	Security Officer's Master Key
SNC	Signing No Cloning
SO	Security Officer
SRK	Secure Recovery Key
STC	Secure Trusted Channel
TUK	Token or Module Unwrapping Key
TVK	Token or Module Variable Key
TWC	Token or Module Wrapping Certificate
TWK	Token or Module Wrapping Key
USK	User's Storage Key

PREFACE

This document considers only the operations and capabilities of the Thales Luna USB HSM 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 is available from the Thales Customer Support Portal at https://supportportal.thalesgroup.com/csm; and
- 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 document describes the security policies enforced by the Thales Luna USB HSM.

1.2 Scope

This document applies to Hardware Version LTK-03-0102 or LTK-03-0103 with Tamper Evident Labels TEL-GEMALTO, TEL-SAFENET, TEL-SAFENET-2, TEL-TRAC and TEL-TRAC 2 and with Firmware Versions 6.10.4, 6.10.7 or 6.10.9.

The security features described in this document apply to the Thales Luna USB HSM only and do not include any feature that may be enforced by the host appliance, client or Thales Luna PED

The Thales Luna USB HSM can be used in one of the following 3 configurations:

- Cloning [CL];
- Signing - No backup [SNB]; or
- Key Export [CKE].

The security policies described in this document apply to the Password Authentication (Level 2) configuration of the Thales Luna USB HSM only and do not include any security policy that may be enforced by the host appliance or server.

1.3 Validation Overview

The cryptographic module meets the following levels for FIPS 140-2 as summarized in the table below:

Table 1: FIPS 140-2 Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2

Security Requirements Section	Level
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2
Cryptographic Module Security Policy	2

2 Security Policy Model Introduction

2.1 Functional Overview

The Thales Luna USB HSM is a multi-chip standalone hardware cryptographic module in the form of a small desktop device that connects to a computer workstation or server via USB. The cryptographic module is contained within a secure enclosure that provides physical resistance to tampering and response if the enclosure is opened. The cryptographic boundary of the module is defined to encompass all components inside the secure enclosure. Figure 2-1 depicts the Thales Luna USB HSM cryptographic module; Figure 2-2 depicts the Thales Luna USB HSM cryptographic boundary.

The module is explicitly configured to operate in either FIPS Level 2 or FIPS Level 3 mode, and may be configured to operate in a non-FIPS mode of operation. Configuration in FIPS mode enforces the use of FIPS-approved algorithms only. Configuration in FIPS Level 2 mode requires the use of passwords for user authentication. Note that selection of FIPS or non-FIPS mode of operation occurs at initialization of the cryptographic module, and cannot be changed during normal operation without zeroizing the module's non-volatile memory.

The cryptographic module is accessed (electrically) via the USB communications interface (located at the back of the device) with the host computer. A USB port, which is provided at the front of the device, will be used to support future enhancements / functionality. 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 interface. A module may host multiple user definitions or "partitions" that are cryptographically separated and are presented as "virtual tokens" to user applications. Each partition must be separately authenticated in order to make it available for use.

This Security Policy is specifically written for the Thales Luna USB HSM in a Password Authentication (FIPS Level 2) configuration.

Figure 2-1. Thales Luna USB HSM

Figure 2-2. Thales Luna USB Cryptographic Boundary (with front bezel removed)

2.1.1 Assets to be Protected

The module is designed to protect the following assets:

- User-generated private keys;
- User-generated secret keys;
- Cryptographic services; and
- Module security critical parameters.

2.1.2 Operating Environment

The module is assumed to operate as a key management and cryptographic processing unit connected over USB to a security appliance that may operate in a TCP/IP network environment. The host appliance may be used in an internal network environment when key management security is a primary requirement. It may also be deployed in environments where it is used primarily as a cryptographic accelerator, in which case it will often be connected to external networks. It is assumed that the appliance includes an internal host computer that runs a suitably secured operating system, with an interface for use by locally connected or remote administrators and an interface to provide access to the module's cryptographic functions by application services running on the host computer. It is also assumed that only known versions of the application services are permitted to run on the internal host computer of the appliance.

It is assumed that trained and trustworthy administrators are responsible for the initial configuration and ongoing maintenance of the appliance and the cryptographic module.

It is assumed that physical access to the cryptographic module will be controlled, and that connections will be controlled either by accessing the module via a direct local connection or by accessing it via remote connections controlled by the host operating system and application service.

3 Security Policy Model Description

This section provides a narrative description of the security policy enforced by the module in its most general form. It is intended both to state the security policy enforced by the module and to give the reader an overall understanding of the security behaviour of the module. The detailed functional specification for the module is provided elsewhere.

The security behaviour of the cryptographic module is governed by the following security policies:

- Operational Policy;
- Identification and Authentication Policy;
- Access Control Policy;
- Cryptographic Material Management Policy;
- Firmware Security Policy; and
- Physical Security Policy.

These policies complement each other to provide assurance that cryptographic material is securely managed throughout its life cycle and that access to other data and functions provided by the product is properly controlled. Configurable parameters that determine many of the variable aspects of the module's behaviour are specified by the higher level Operational Policy implemented at two levels: the cryptographic module as a whole and the individual partition. This is described in section 3.1.1.

The Identification and Authentication policy is crucial for security enforcement and it is described in section 3.3. The access control policy is the main security functional policy enforced by the module and is described in section 3.3.3, which also describes the supporting object re-use policy. Cryptographic Material Management is described in section 3.4. Firmware security, physical security and fault tolerance are described in sections 3.6 through 3.10.

3.1.1 Operational Policy

The module employs the concept of the Operational Policy to control the overall behaviour of the module and each of the partitions within. At each level, either the module or the partition is assigned a fixed set of "capabilities" that govern the allowed behaviour of the module or individual partition. The Security Officer (SO) establishes the Operational Policy by enabling/disabling or refining the corresponding policy elements to equate to or to be more restrictive than the pre-assigned capabilities.

The set of configurable policy elements is a proper subset of the corresponding capability set. That is, not all elements of the capability set can be refined. Which of the capability set elements have corresponding policy set elements is pre-determined based on the "personality" of the partition or manufacturing restrictions placed on the module. For example, the module capability setting for "domestic algorithms and key sizes available" does not have a corresponding configurable policy element.

There are also several fixed settings that do not have corresponding capability set elements. These are elements of the cryptographic module's behaviour that are truly fixed and, therefore, are not subject to configuration by the SO. The specific settings[1] are the following:

- Allow/disallow non-sensitive secret keys – fixed as disallow;
- Allow/disallow non-sensitive private keys – fixed as disallow;
- Allow/disallow non-private secret keys – fixed as disallow;
- Allow/disallow non-private private keys – fixed as disallow;
- Allow/disallow secret key creation through the create objects interface – fixed as disallow; and
- Allow/disallow private key creation through the create objects interface – fixed as disallow.

Further, policy set elements can only refine capability set elements to more restrictive values. Even if an element of the policy set exists to refine an element of the capability set, it may not be possible to assign the policy set element to a value other than that held by the capability set element. Specifically, if a capability set element is set to allow, the corresponding policy element may be set to either enable or disable. However, if a capability set element is set to disallow, the corresponding policy element can only be set to disable. Thus, an SO cannot use policy refinement to lift a restriction set in a capability definition.

3.1.2 Module Capabilities

The following is the set of capabilities supported at the module level:

- Allow/disallow non-FIPS algorithms available;
- Allow/disallow password authentication (allowed and must be enabled in Level 2 configuration);
- Allow/disallow partition groups;
- Allow/disallow cloning;
- Allow/disallow masking;
- Allow/disallow unmasking;
- Allow/disallow Korean algorithms;
- Allow/disallow SO reset of partition PIN;
- Allow/disallow network replication;
- Allow/disallow forcing change of User authentication data; and
- Allow/disallow Acceleration

[1] The nomenclature used for these settings is based on PKCS#11.

3.1.3 Partition Capabilities

The following is the set of capabilities supported at the partition level. All capability elements described as “allow/disallow some functionality” are Boolean values where false (or “0”) equates to disallow the functionality and true (or “1”) equates to allow the functionality. The remainder of the elements are integer values of the indicated number of bits.

- Allow/disallow changing of certain key attributes once a key has been created;
- Allow/disallow multipurpose keys;
- Allow/disallow operation without RSA blinding;
- Allow/disallow signing operations with non-local keys;
- Allow/disallow raw RSA operations;
- Allow/disallow private key wrapping;
- Allow/disallow private key unwrapping;
- Allow/disallow secret key wrapping;
- Allow/disallow secret key unwrapping;
- Allow/disallow RSA signing without confirmation; and
- Number of failed Partition User logins allowed before partition is locked out/cleared (default is 10; SO can configure it to be 3 <= N <= 10).

The following capabilities are configurable only if the corresponding capability/policy is allowed and enabled at the module level:

- Allow/disallow private key cloning;
- Allow/disallow secret key cloning;
- Allow/disallow private key masking;
- Allow/disallow secret key masking;
- Allow/disallow private key unmasking; and
- Allow/disallow secret key unmasking.

The following tables summarize the module and partition capabilities, showing typical capability settings for Thales Luna USB HSM used in the following configurations (An X indicates the default capability setting for each configuration of the module. Greyed-out rows indicate that the corresponding capability setting is not used as a default for any module configuration.):

- Key Export (CKE);
- Signing – No Backup (SNB); and
- Cloning (CL).

Table 3-1. Module Capabilities and Policies

Description	Capability	SNB	CKE	CL	Policy	Comments
Non-FIPS algorithms available	Allow	X	X	X	Enable Disable	SO can configure the policy to enable or disable the availability of non-FIPS algorithms at the time the cryptographic module is initialized.
	Disallow				Disable	The cryptographic module must operate using FIPS-approved algorithms only. Must be disabled in FIPS mode
Password authentication	Allow	X	X	X	Enable Disable	SO can configure the policy to enable or disable the use of passwords without trusted path for authentication.
	Disallow				Disable	The cryptographic module must operate using the trusted path and module-generated secrets for authentication.
Cloning	Allow		X	X	Enable Disable	SO can configure the policy to enable or disable the availability of the cloning function for the cryptographic module as a whole.
	Disallow	X			Disable	The cryptographic module must operate without cloning.
Masking	Allow				Enable Disable	SO can configure the policy to enable or disable the availability of the masking function for the cryptographic module as a whole.
	Disallow	X	X	X	Disable	The cryptographic module must operate without masking.
Unmasking	Allow	X	X	X	Enable Disable	SO can configure the policy to enable or disable the availability of the unmasking function for the cryptographic module as a whole.
	Disallow				Disable	The cryptographic module must operate without unmasking.
Korean algorithm	Allow				Enable Disable	SO can configure the policy to enable or disable of Korean algorithms for the cryptographic the availability module as a whole.
	Disallow	X	X	X	Disable	The cryptographic module must operate without Korean algorithms.
Partition reset	Allow	X	X	X	Enable Disable	SO can configure the policy to enable a partition to be reset if it is locked as a result of exceeding the maximum number of failed login attempts.
	Disallow				Disable	A partition cannot be reset and must be re-created as a result of exceeding the maximum number of failed login attempts.
					Enable	

Description	Capability	SNB	CKE	CL	Policy	Comments
Network Replication	Allow			**X**	Disable	SO can configure the policy to enable the replication of the module's key material over the network to a second module.
	Disallow	**X**	**X**		Disable	The module cannot be replicated over the network.
Force user PIN change	Allow	**X**	**X**	**X**	Enable Disable	This capability is set prior to shipment to the customer. If enabled, it forces the user to change the PIN upon first login.
	Disallow				Disable	The user is never forced to change PIN on first login.
Acceleration	Allow	**X**	**X**	**X**	Enable Disable	This capability is set prior to shipment to the customer. It allows the use of the onboard crypto accelerator.
	Disallow				Disable	Remote authentication cannot be enabled for the module.

Table 3-2. Partition Capabilities and Policies

Description	Prerequisite	Capability	SNB	KE	CL	Policy	Comments
Multipurpose keys	N/A	Allow	**X**	**X**	**X**	Enable Disable	SO can configure the policy to enable the use of keys for more than one purpose, e.g., an RSA private key could be used for digital signature and for decryption for key transport purposes.
		Disallow				Disable	Keys can only be used for a single purpose.
Change attributes	N/A	Allow	**X**	**X**	**X**	Enable Disable	SO can configure the policy to enable changing key attributes.
		Disallow				Disable	Key attributes cannot be changed.
Operate without RSA blinding	N/A	Allow	**X**	**X**	**X**	Enable Disable	SO can configure the use of blinding mode for RSA operations. Blinding mode is used to defeat timing analysis attacks on RSA digital signature operations, but it also imposes a significant performance penalty on the signature operations.
		Disallow				Disable	Blinding mode is not used for RSA operations.
Signing with non-local keys	N/A	Allow	**X**	**X**	**X**	Enable Disable	SO can configure the ability to sign with externally-generated private keys that have been imported into the partition.
		Disallow				Disable	Externally-generated private keys cannot be used for signature operations.
Raw RSA operations	N/A	Allow	**X**	**X**	**X**	Enable Disable	SO can configure the ability to use raw (no padding) format for RSA encrypt/decrypt operations for key transport purposes.
		Disallow				Disable	Raw RSA cannot be used.
Private key wrapping	N/A	Allow		**X**		Enable Disable	SO can configure the ability to wrap private keys for export.

Description	Prerequisite	Capability	SNB	KE	CL	Policy	Comments
		Disallow	**X**		**X**	Disable	Private keys cannot be wrapped and exported from the partition.
Private key unwrapping	N/A	Allow	**X**	**X**	**X**	Enable	SO can configure the ability to unwrap private keys and import them into the partition.
						Disable	
		Disallow				Disable	Private keys cannot be unwrapped and imported into the partition.
Secret key wrapping	N/A	Allow	**X**	**X**	**X**	Enable	SO can configure the ability to wrap secret keys and export them from the partition.
						Disable	
		Disallow				Disable	Secret keys cannot be wrapped and exported from the partition.
Secret key unwrapping	N/A	Allow	**X**	**X**	**X**	Enable	SO can configure the ability to unwrap secret keys and import them into the partition.
						Disable	
		Disallow				Disable	Secret keys cannot be unwrapped and imported into the partition.
Private key cloning	Cloning enabled, Trusted path authentication enabled	Allow			**X**	Enable	SO can configure the ability to clone private keys from one module and partition to another.
						Disable	
		Disallow	**X**	**X**		Disable	Private keys cannot be cloned.
Secret key cloning	Cloning enabled, Trusted path authentication enabled	Allow		**X**	**X**	Enable	SO can configure the ability to clone secret keys from one module and partition to another.
						Disable	
		Disallow	**X**			Disable	Secret keys cannot be cloned.
						Enable	

Description	Prerequisite	Capability	SNB	KE	CL	Policy	Comments
Private key masking	Masking enabled	Allow				Disable	SO can configure the ability to mask private keys for storage outside the partition.
		Disallow	**X**	**X**	**X**	Disable	Private keys cannot be masked for storage outside the partition.
Secret key masking	Masking enabled	Allow				Enable	SO can configure the ability to mask secret keys for storage outside the partition.
						Disable	
		Disallow	**X**	**X**	**X**	Disable	Secret keys cannot be masked for storage outside the partition.
Private key unmasking	Secret key cloning enabled	Allow		**X**	**X**	Enable	This setting allows unmasking of private keys.
						Disable	
		Disallow				Disable	Private keys cannot be unmasked
Secret key unmasking	Secret key cloning enabled	Allow		**X**	**X**	Enable	This setting allows unmasking of secret keys.
						Disable	
		Disallow				Disable	Secret keys cannot be unmasked
Minimum / maximum password length	User password authentication enabled	7-16 characters				Configurable	The SO can configure the minimum password length for Level 2 modules, but minimum length must always be >= 7.
Number of failed Partition User logins allowed	N/A	Minimum:1, Maximum: 10				Configurable	The SO can configure; default maximum value is 10.

3.2 Description of Operator, Subject and Object

3.2.1 Operator

An operator is defined as an entity that acts to perform an operation on a module. An operator may be directly mapped to a responsible individual or organization, or it may be mapped to a composite of a responsible individual or organization plus an agent (application program) acting on behalf of the responsible individual or organization.

In the case of a Certification Authority (CA), for example, the organization may empower one individual or a small group of individuals acting together to operate a cryptographic module as part of the company's service. The operator might be that individual or group, particularly if they are interacting with a module locally. The operator might also be the composite of the individual or group, who might still be present locally to a module, plus the CA application running on a network-attached host computer.

3.2.2 Roles

In a Level 2 configuration (Password Authentication), the cryptographic module supports the following authenticated roles: the Security Officer (SO), Audit Officer, and Partition User. It also supports one unauthenticated operator role, the Public User, primarily to permit access to status information and diagnostics before authentication.

The SO is a privileged role, which exists only at the module level, whose primary purpose is to initially configure a module for operation and to perform security administration tasks such as partition creation.

The Audit Officer is a privileged role, which exists only at the module level to initialize, configure, and manage secure audit logging. Only the Audit Officer can initialize, configure and manage the secure audit logging feature. This allows for a separation of duties between an Audit Officer and the other roles (e.g., SO, Partition User) that the Audit Officer is auditing – preventing administrative and user personnel from tampering with the log files and preventing the Audit Officer from performing administrative tasks or from accessing keys.

The Partition User is the key management and user role for the partition. The SO, by disabling the "User Key Management" policy (see Table 3-1), can limit the Partition User to a read-only role that limits the operator to performing cryptographic operations only.

For an operator to assume any role other than Public User, the operator must be identified and authenticated. The following conditions must hold in order to assume one of the authenticated roles:

- No operator can assume the Audit Officer, Partition User or Security Officer role before identification and authentication;
- No identity can assume more than one authenticated roles at the same time. e.g., Partition User, plus the Security Officer role, or Audit Officer, plus Security Officer.

For additional information regarding roles and authorized services, please refer to Table 5-1 and Table 5-3.

3.2.3 Account Data

The module maintains the following User and SO account data:

> Partition ID or SO ID number;

> Partition User encrypted or SO encrypted authentication data (checkword);

> Partition User authentication challenge secret (one for each role, as applicable); and

> Partition User locked out flag.

An authenticated User is referred to as a Partition User. The ability to manipulate the account data is restricted to the SO and the Partition User. The specific restrictions are as described below:

> Only the Security Officer role can create (initialize) and delete the following security attributes:

- Partition ID; and
- Checkword.

> If “SO can reset partition PIN” is allowed and enabled, the SO role only can modify the following security attribute:

- Locked out flag for Partition User.

> Only the Partition User can modify the following security attribute:

- Checkword for Partition User.

> Only the Security Officer role can change the default value, query, modify and delete the following security attribute:

- Checkword for Security Officer.

3.2.4 Subject

For the purposes of this security policy, the subject is defined to be a module session. The session provides a logical means of mapping between applications connecting to a module and the processing of commands within a module. Each session is tracked by the Session ID, the Partition ID and the Access ID, which is a unique ID associated with the application’s connection. It is possible to have multiple open sessions with a module associated with the same Access ID/Partition ID combination. It is also possible for a module to have sessions opened for more than one Partition ID or have multiple Access IDs with sessions opened on a module. Applications running on remote host systems that require data and cryptographic services from a module must first connect via the communications service within the appliance, which will establish the unique Access ID for the connection and then allow the application to open a session with one of the partitions within a module. A local application (e.g., command line administration interface) will open a session directly with the appropriate partition within a module without invoking the communications service.

3.2.5 Operator - Subject Binding

An operator must access a partition through a session. A session is opened with a partition in an unauthenticated state and the operator must be authenticated before any access to cryptographic functions and Private objects within the partition can be granted. Once the operator is successfully identified and authenticated, the session state becomes authenticated and is bound to the Partition

User represented by the Partition ID. Any other sessions opened with the same Access ID/Partition ID combination will share the same authentication state and be bound to the same Partition User.

3.2.6 Object

An object is defined to be any formatted data held in volatile or non-volatile memory on behalf of an operator. For the purposes of this security policy, the objects of primary concern are private (asymmetric) keys and secret (symmetric) keys.

3.2.7 Object Operations

Object operations may only be performed by a Partition User. The operations that may be performed are limited by the role associated with the user's login state, see section 3.3.3. New objects can be made in several ways. The following list identifies operations that produce new objects:

- Create;
- Copy;
- Generate;
- Unwrapping; and
- Derive.

Existing objects can be modified and deleted. The values of a subset of attributes can be changed through a modification operation. Objects can be deleted through a destruction operation. Constant operations do not cause creation, modification or deletion of an object. These constant operations include:

- Query an object's size;
- Query the size of an attribute;
- Query the value of an attribute;
- Use the value of an attribute in a cryptographic operation;
- Search for objects based on matching attributes;
- Cloning an object;
- Wrapping an object; and
- Masking and unmasking an object.

Secret keys and private keys are always maintained as Sensitive objects and, therefore, they are permanently stored with the key value encrypted to protect its confidentiality. Key objects held in volatile memory do not have their key values encrypted, but they are subject to active zeroization in the event of a module reset or in response to a tamper event. For additional information about the clearing of sensitive data, see Section 3.11. Operators are not given direct access to key values for any purpose.

3.3 Identification and Authentication

3.3.1 Authentication Data Generation and Entry

The module requires that Partition Users, the Audit Officer, and the SO be authenticated by proving knowledge of a secret shared by the operator and the module. The FIPS mode is determined when the module is initialized: a module that is to support Level 2 mode must be initialized using a password to define the SO authentication data.

For a module operating in FIPS Level 2 mode, the SO must enable the “User password authentication” (implies that the trusted path authentication is disallowed or disabled). The SO defines a user password when a partition is created. The minimum length of the password must always be equal to or greater than 7 characters, and up to 16 characters.

3.3.2 Limits on Login Failures

The module also implements a maximum login attempts policy. The policy differs for an SO authentication data search, a Partition User authentication data search, or an Audit Officer data search.

In the case of an SO authentication data search:

> If three (3) consecutive SO logon attempts fail, a module is zeroized.

In the case of a Partition User authentication data search, one of two responses will occur, depending on the partition policy:

> If “Partition reset” is Allowed and Enabled, then if “n” (“n” is set by the SO at the time the cryptographic module is initialized) consecutive operator logon attempts fail, the module flags the event in the Partition User’s account data, locks the Partition User and clears the volatile memory space. The SO must unlock the partition in order for the Partition User to resume operation.

> If “Partition reset” is not Allowed or not Enabled, then if “n” consecutive Partition User logon attempts via the physical trusted path fail, the module will erase the partition. The SO must delete and re-create the partition. Any objects stored in the partition, including private and secret keys, are permanently erased.

In the case of an Audit Officer data search:

> If three consecutive Audit Officer logon attempts fail, the Audit Officer account will be locked for 60 seconds. After the 60 second lockout timeout, the Audit Officer may attempt to logon to the module again.

3.3.3 Access Control

The Access Control Policy is the main security function policy enforced by a module. It governs the rights of a subject to perform privileged functions and to access objects stored in a module. It covers the object operations detailed in section 3.2.7.

A subject’s access to objects stored in a module is mediated on the basis of the following subject and object attributes:

> Subject attributes:

- Session ID;
- Access ID and Partition ID associated with session; and
- Session authentication state (binding to authenticated Partition identity and role).

> Object attributes:

- **Owner.** A Private object is owned by the Partition User associated with the subject that produces it. Ownership is enforced via internal key management;
- **Private.** If True, the object is Private. If False, the object is Public;
- **Sensitive.** If True, object is Sensitive. If False, object is Non-Sensitive;
- **Extractable[2].** If True, object may be extracted. If False, object may not be extracted; and
- **Modifiable.** If True, object may be modified. If False, object may not be modified.

Objects are labelled with a number corresponding to their partition and are only accessible by a subject associated with the owning Partition ID. Only generic data and certificate objects can be non-sensitive. Private key and secret key objects are always created as Sensitive, Private objects. Sensitive objects are encrypted using the partition's secret key to prevent their values from ever being exposed to external entities. Private objects can only be used for cryptographic operations by a logged in Partition User. Key objects that are marked as extractable may be exported from a module using the Wrap operation if allowed and enabled in the partition's policy set. Table 3-3 summarizes the object attributes used in Access Control Policy enforcement.

Table 3-3. Object Attributes Used in Access Control Policy Enforcement

Attribute	Values	Impact
PRIVATE	TRUE – Object is private to (owned by) the operator identified as the Access Owner when the object is created.	Object is only accessible to subjects (sessions) bound to the operator identity that owns the object.
	FALSE – Object is not private to one operator identity.	Object is accessible to all subjects associated with the partition in which the object is stored.
SENSITIVE	TRUE – Attribute values representing plaintext key material are not permitted to exist (value encrypted).	Key material is stored in encrypted form.
	FALSE – Attribute values representing plaintext data are permitted to exist.	Plaintext data is stored with the object and is accessible to all subjects otherwise permitted access to the object.
MODIFIABLE	TRUE – The object's attribute values may be modified.	The object is "writeable" and its attribute values can be changed during a copy or set attribute operation.
	FALSE – The object's values may not be modified.	The object can only be read and only duplicate copies can be made.
EXTRACTABLE	TRUE – Key material stored with the object may be extracted from the Thales cryptographic module using the Wrap operation.	The ability to extract a key permits sharing with other crypto modules and archiving of key material.

[2] Extract means to remove the key from the control of the module. This is typically done using the Wrap operation, but the Mask operation is also considered to perform an extraction when cloning is enabled for the container.

Attribute	Values	Impact
	FALSE – Key material stored with the object may not be extracted from the Thales cryptographic module.	Keys must never leave a module's control.

The module does not allow any granularity of access other than owner or non-owner (i.e., a Private object cannot be accessible by two Partition Users and restricted to other Partition Users). Ownership of a Private object gives the owner access to the object through the allowed operations but does not allow the owner to assign a subset of rights to other operators. Allowed operations are those permitted by the cryptographic module and Partition Capability and Policy settings.

The policy is summarized by the following statements:

> A subject may perform an allowed operation on an object if the object is in the partition with which the subject is associated and one of the following two conditions holds:
  - The object is a "Public" object, i.e., the PRIVATE attribute is FALSE; or
  - The subject is bound to the Partition User that owns the object.
> Allowed operations are those permitted by the object attribute definitions within the constraints imposed by the module and Partition Capability and Policy settings.

3.3.4 Object Protection

The module cryptographically protects the values of sensitive objects stored in its internal flash memory. Sensitive values are protected using AES 256 bit encryption with three different keys – each having a separate protection role. The three keys used to protect sensitive object values are the following:

> User Storage Key (USK)/Security Officer Master Key (SMK) – this key is created by the cryptographic module when the User or SO is created. It is used to maintain cryptographic separation between users' keys.
> Master Tamper Key (MTK) – this key is securely stored in the battery-backed RAM. It encrypts keys as they are generated to ensure that they can only be used by the co-processor itself or with authorization from it.
> Key Encryption Key (KEK) – this key is stored in battery-backed RAM in the module. It also encrypts all sensitive object values and is used to provide the "decommissioning" feature. The KEK is erased in response to an external decommission signal. 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.

3.3.5 Object Re-use

The access control policy is supported by an object re-use policy. The object re-use policy requires that the resources allocated to an object be cleared of their information content before they are re-allocated to a different object.

3.3.6 Privileged Functions

The module shall restrict the performance of the following functions to the SO role only:

- Module initialization;
- Partition creation and deletion;
- Configuring the module and partition policies;
- Module zeroization; and
- Firmware update.

3.4 Cryptographic Material Management

Cryptographic material (key) management functions protect the confidentiality of key material throughout its life cycle. The FIPS PUB 140-2 approved key management functions provided by the module are the following:

- Deterministic Random Bit Generation (DRBG) in accordance with NIST SP 800-90A section 10.2.1.
- Cryptographic key generation in accordance with the following indicated standards:
  - RSA 2048-4096 bits key pairs in accordance with FIPS PUB 186-4 and ANSI X9.31.
  - Triple-DES 112 bits and 168 bits (SP 800-67).
  - AES 128, 192, 256 bits (FIPS PUB 197).
  - DSA 2048 and 3072 bit key pairs in accordance with FIPS PUB 186-4.
  - Elliptic Curve key pairs (curves in accordance with SP 800-57) in accordance with FIPS PUB 186-4.
  - Diffie-Hellman key pairs.
  - Key Derivation in accordance with NIST SP 800-108 (Counter mode).
- Diffie-Hellman (2048 bits) (key agreement; key establishment methodology provides 112 bits of encryption strength).
- EC Diffie-Hellman (ECDH) (curves in accordance with SP 800-57) key establishment in accordance with NIST SP 800-56A.
- Symmetric key unwrap: Triple-DES 168 bits and AES 128, 192 and 256 bits in accordance with PKCS #11 (key transport provides 112 bits of security strength with Triple-DES and between 128 and 256 bits of security strength with AES).
- Asymmetric key wrap / unwrap: RSA 2048 – 4096 (PKCS #1 V1.5 and OAEP) (key transport provides between 112 and 152 bits of security strength).
- Encrypted key storage (using AES 256 bit encryption) and key access following the PKCS #11 standard.
- Destruction of cryptographic keys is performed in one of three ways as described below in accordance with the PKCS #11 and FIPS PUB 140-2 standards:
  - An object on a Luna cryptographic module that is destroyed using the PKCS #11 function C_DestroyObject is marked invalid and remains encrypted with the Partition User's key or a Luna cryptographic module’s general secret key until such time as its memory locations

(flash or RAM) are re-allocated for additional data on a Luna cryptographic module, at which time they are purged and zeroized before re-allocation.

- Objects on a Luna cryptographic module that are destroyed as a result of authentication failure are zeroized (all flash blocks in the Partition User's memory turned to 1's). If it is an SO authentication failure, all flash blocks used for key and data storage on a Luna cryptographic module are zeroized.
- Objects on a Luna cryptographic module that are destroyed through C_InitToken (the SO-accessible command to initialize a Luna cryptographic module available through the API) are zeroized, along with the rest of the flash memory being used by the SO and Partition Users.

Keys are always stored as secret key or private key objects with the Sensitive attribute set. The key value is, therefore, stored in encrypted form using the owning Partition User's Storage Key (USK) and the Master Tamper Key (MTK) stored in the battery-backed RAM. Access to keys is never provided directly to a calling application. A handle to a particular key is returned that can be used by the application in subsequent calls to perform cryptographic operations.

Private key and secret key objects may be imported into a module using the Unwrap, Unmask (if cloning and unmasking are enabled at the module level) or Derive operation under the control of the Access Control Policy. Any externally-set attributes of keys imported in this way are ignored by a module and their attributes are set by a module to values required by the Access Control Policy.

3.4.1 Key Cloning

Key cloning is a Luna product feature that uses a one-time 3-key Triple-DES 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 Triple-DES session encrypting key is obtained by combining the 24-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.

3.4.2 Key Mask/Unmask

Key masking is a Thales product feature that uses a 256-bit AES key, which is unique to the module, to encrypt a key object for output in a way that ensures the key can only be imported, by unmasking, into the module from which it originally came or one that has been initialized to contain the same "master" key for the module. The key mask operation takes a key handle as input and uses the module's validated AES implementation to create the masked key output.

The key unmask operation takes a masked (encrypted) key object as input, performs the necessary decryptions inside the module and returns a handle to the imported key.

Note that for both mask and unmask 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.

3.4.3 Key Wrap/Unwrap

The key wrap operation encrypts a key value for output, using either an RSA public key (only if wrapping a symmetric key) or a symmetric key to wrap either another symmetric key or an asymmetric private key.

The unwrap operation takes as input an encrypted key value and a handle to the key that was originally used to do the wrapping. It decrypts the key value, 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.

3.5 Cryptographic Operations

Because of its generic nature, the module's cryptographic co-processor and firmware support a wide range of cryptographic algorithms and mechanisms. The approved cryptographic functions and algorithms that are relevant to the FIPS 140-2 validation are the following:

- Symmetric encryption/decryption: Triple-DES 112 bits and 168 bits (SP 800-67).
- Symmetric encryption/decryption: AES 128, 192, 256 bits (FIPS PUB 197).
- Signature generation (FIPS PUB 186-4): RSA 2048-3072 bits (PKCS #1 V1.5) with SHA- 224, SHA-256, SHA-384, SHA-512, RSA 2048-3072 bits (PSS) with SHA-224, SHA-256, SHA-384, SHA-512, RSA 2048-3072 bits (ANSI X9.31) with SHA-224, SHA-256, SHA-384 and SHA-512; DSA 2048-3072 bits with SHA-224, SHA-256; ECDSA with SHA-224, SHA- 256, SHA-384, SHA-512.
- Signature verification (FIPS PUB 186-4): RSA 1024-3072 bits (PKCS #1 V1.5) with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RSA 1024-3072 bits (PSS) with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RSA 1024-3072 bits (ANSI X9.31) with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512; DSA 1024-3072 bits with SHA-1, SHA-224, SHA-256; ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
- Signature verification (FIPS PUB 186-2): RSA 1024-4096 bits with SHA-1, SHA-224, SHA- 256, SHA-384, SHA-512; DSA 1024 bits with SHA-1.
- Hash generation SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 180-4).
- Keyed hash generation HMAC using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 198-1).
- Message authentication Triple-DES MAC (FIPS PUB 113) and CMAC (NIST SP 800-38B).
- Deterministic Random Bit Generation (DRBG) (NIST SP 800-90A section 10.2.1).

Table 3-4. Approved Security Functions for SafeXcel 3120

Approved Security Functions	Certificate No.
Symmetric Encryption/Decryption	
AES: (ECB, CBC, GCM); Encrypt/Decrypt; Key Size = 128, 192, 256)	2664
Triple-DES: (TECB, TCBC); Encrypt/Decrypt KO 1,2)	1598
Hashing	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	2237

Message Authentication Code	
HMAC-SHA-1[19], HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	1655
Triple-DES MAC (based on Certificate No. 1598)	Vendor Affirmed
Asymmetric	
RSA: **FIPS186-2:** ALG[ANSIX9.31]; SIG (ver) (MOD: 1024, 1536, 2048, 3072, 4096); ALG[RSASSA-PKCS1_V1_5]; SIG(ver); (MOD: 1024, 1536, 2048, 3072, 4096); ALG[RSASSA-PSS]; SIG (ver) (MOD: 1024, 1536, 2048, 3072, 4096);	1369
DSA: **FIPS186-4: PQG(gen):** [(2048, 224) SHA(224); (2048,256) SHA(256); (3072,256) SHA(256);] **KEYGEN:** [(2048,224); (2048,256) (3072,256)] **SIG(gen):** [(2048,224) SHA(224); (2048,256) SHA(256); (3072,256) SHA(256);] **SIG(ver):** [(1024,160) SHA(1); (2048,224) SHA(224); (2048,256) SHA(256); (3072,256) SHA(256);]	804
ECDSA: **FIPS186-4: PKG**: CURVES (P-224; P-256; P-384) Testing Candidates **SIG(gen):** CURVES (P-224: (SHA-224) P-256: (SHA-224, 256); P-384: (SHA-224, 256, 384) **SIG(ver):** CURVES (P-192: (SHA-1); P-224: (SHA-1, 224); P-256: (SHA-1, 224, 256) P-384: (SHA-1, 224, 256, 384)	461
Random Number Generation	
NIST SP 800-90A DRBG (CTR) AES-256	428

Table 3-5. Approved Security Functions for Firmware Implementation

Approved Security Functions	**Certificate No.**
Symmetric Encryption/Decryption	
AES: (ECB, CBC, OFB, CFB8, CFB128, GCM); Encrypt/Decrypt; Key Size = 128, 192, 256)	2668
Triple-DES: (TECB, TCBC, OFB, CFB8, CFB64); Encrypt/Decrypt KO 1,2) [20]	1600
Hashing	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	2241
Message Authentication Code	
HMAC-SHA-1[21], HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	1659
Triple-DES MAC (based on Certificate No. 1600)	Vendor Affirmed

AES CMAC (Key Sizes Tested: 128 192 256)	2668
Asymmetric	
RSA: **FIPS186-2:** [ANSIX9.31]; SIG (ver) (MOD: 1024, 1536, 2048, 3072, 4096); [RSASSA-PKCS1_V1_5]; SIG(ver); (MOD: 1024, 1536, 2048, 3072, 4096); SHA(1, 224, 256, 384, 512); [RSASSA-PSS]; SIG(ver); (MOD: 1024, 1536, 2048, 3072, 4096) SHA(1, 224, 256, 384, 512)) **FIPS 186-4: KEY(gen):** [ANSIX9.31] (MOD: 2048, 3072); SIG(gen) (MOD: 2048 SHA(224, 256, 384, 512); 3072); SIG (ver) (MOD: 1024 SHA(1, 224, 256, 384, 512); 2048 SHA(1, 224, 256, 384, 512); 3072); 512)); [RSASSA-PKCS1_V1_5]; SIG(gen) (MOD: 2048 SHA(224, 256, 384, 512); 3072); SIG(ver); (MOD: 1024 SHA(1, 224, 256, 384, 512); (2048 SHA(1, 224, 256, 384, 512); 3072; 512); ALG[RSASSA-PSS]; SIG(gen) (MOD: 2048 SHA(224, 256, 384, 512); 3072); SHA(224, 256, (MOD: 1024 SHA(1, 224, 256, 384, 512), 2048 SHA(1, 224, 256, 384, 512), 3072 SHA(1, 224, 256, 384, 512))	1372
DSA: **FIPS186-4:** **KEYGEN:** [(2048, 224); (2048,256); (3072,256)] **SIG(gen):** [(2048, 224) SHA(224); (2048,256) SHA(256); (3072,256) SHA(256)] SIG(ver): [(1024,160) SHA(1); (2048, 224) SHA(224); (2048,256) SHA(256); (3072,256) SHA(256)]	808
ECDSA: **FIPS186-4: PKG:** CURVES(P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-Candidates **SIG(gen):** CURVES(P-224: (SHA-224, 256, 384, 512) P-256: (SHA-224, 256, 384, 512) P-384: 512) P-521: (SHA-224, 256, 384, 512) K-233: (SHA-224, 256, 384, 512) K-283: (SHA-224, 256, 384, 512) K-409: (SHA-224, 256, 384, 512) K-571: (SHA-224, 256, 384, 512) B-233 (SHA-224, 256, 384, 512) B-283: (SHA-224, 256, 571: (SHA-224, 256, 384, 512) **SIG(ver):** CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, (SHA-1, 224, 256, 384, 512) K-571: (SHA-1, 224, 256, 384, 512) B-163: (SHA-1, 224, 256, 384, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-384, 512)	464
Key Agreement Scheme	
ECC: (ASSURANCES) **SCHEMES [Ephemeral Unified** (KARole(s): Initiator / Responder) ((EB: P-224 SHA224 SHA256 SHA384 SHA512) (EC: P-256 SHA256 SHA384 SHA512) (ED: P- 384 SHA384 SHA512) (EE: P-521)] **[OnePassDH (No_KC:** [N/A]) (KARole(s): Initiator / Responder) (EB: P-224 SHA224 SHA256 SHA384 SHA512 HMAC) (EC: P-256 SHA256 SHA384 SHA512 HMAC) (ED: P-384 SHA384 SHA512 HMAC) (EE: P-521)]	44

Key Derivation	
NIST SP 800-108 (Counter Mode)	15

Table 3-6. Allowed Security Functions for Firmware Implementation

Allowed Security Functions
Key Agreement
Diffie-Hellman (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength)
Key Transport
RSA (key wrapping; key establishment methodology provides between 112 and 152 bits of encryption strength)
AES (key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)
Triple-DES (key unwrapping; key establishment methodology provides 112 bits of encryption strength)

Non-FIPS Approved security functions are not available for use when the module has been configured to operate in FIPS-approved mode, see Section 4.1.

Table 3-7. Non-FIPS Approved Security Functions

Non-FIPS Approved Security Functions
Symmetric Encryption/Decryption
DES
RC2
RC4
RC5
CAST5
SEED
ARIA
Hashing
MD2
MD5
HAS-160
Message Authentication Code
AES MAC (non-compliant)

DES-MAC
RC2-MAC
RC5-MAC
CAST5-MAC
SSL3-MD5-MAC[22]
SSL3-SHA1-MAC[23]
HMAC (Cert #1659, Cert #1655 – non-compliant less than 112 bits of encryption strength)
Asymmetric
KCDSA
RSA X-509
RSA (Cert #1369, Cert #1372 – non compliant less than 112 bits of encryption strength)
DSA (Cert #804, Cert #808 – non-compliant less than 112 bits of encryption strength)
ECDSA (Cert #461, Cert #464 – non-compliant less than 112 bits of encryption strength)
Generate Key
DES
RC2
RC4
RC5
CAST5
SEED
ARIA
GENERIC-SECRET
SSL PRE-MASTER[24]
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)
AES (key wrapping)
Triple-DES (key wrapping)
Entropy Source
Hardware Random Number Generator (free-running local oscillators)

3.6 Self-Tests

The module provides self-tests on power-up and on request to confirm the firmware integrity, and to check the random number generator and each of the implemented cryptographic algorithms.

Table 3-8. Module Self-Tests

Test	When Performed	Where Performed	Indicator
Boot loader performs a SHA-1 integrity check of the firmware prior to firmware start	Power-on	Firmware	Module halt[3]
Boot loader performs ECDSA integrity check of the binary running on the 3120.	Power-on	Hardware	Module halt
ECDSA integrity check of the binary running on the hardware.	Power-on	Hardware	Module halt
DRBG Instantiate Function Known Answer Test (KAT)	Power-on	Hardware	Module halt
DRBG Generate Function KAT	Power-on	Hardware	Module halt
DRBG Reseed Function KAT	Power-on	Hardware	Module halt
DRBG Uninstantiate Function KAT	Power-on	Hardware	Module halt
Triple-DES KATs (e / d)	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt[4]
SHA-1 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
SHA-224 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
SHA-256 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
SHA-384 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt

[3] Details of the failure can be obtained from the dual-port following a module halt.
[4] An error message is output, the cryptographic module halts, and data output is inhibited.

Test	When Performed	Where Performed	Indicator
SHA-512 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
HMAC SHA-1 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
HMAC SHA-224 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
HMAC SHA-256 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
HMAC SHA-384 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
HMAC SHA-512 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
RSA sig-gen KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
RSA sig-ver KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
DSA sig-gen KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
DSA sig-ver KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
Diffie-Hellman KAT	Power-on/Request	Firmware	Module halt / Error - Halt
AES KATs (e /d)	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
AES-GCM KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
ECDH KAT	Power-on/Request	Firmware	Module halt / Error - Halt
ECDSA sig-gen KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
ECDSA sig-ver KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
KDF KAT	Power-on/Request	Firmware	Module halt / Error - Halt
DRBG conditional tests	Continuous	Firmware / Hardware	Error - Halt
HRNG conditional tests	Continuous	Firmware / Hardware	Error - Halt
RSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware / Hardware	Error
DSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware / Hardware	Error

Test	When Performed	Where Performed	Indicator
ECDSA – Pair-wise consistency test (asymmetric key pairs)	On generation	Firmware / Hardware	Error
Firmware load test (4096-bit RSA sig ver)	On firmware update load	Firmware	Error – module will continue with existing firmware

While the module is running Power-On Self Tests (POST) all interfaces are disabled until the successful completion of the self-tests.

3.7 Firmware Security

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

The module shall not allow external software to be loaded inside its boundary. Only properly formatted firmware may be loaded. The communication of initial or updated firmware to a target module shall be initiated by a Thales module dedicated to that function. Firmware shall be digitally signed using the Thales Manufacturing signature key and encrypted using a secret key that can be derived (based on an internally held secret key) by the receiving module for decryption. RSA (4096 bits) PKCS #1 V1.5 with SHA-256 is used as the approved signature method. The unencrypted firmware must not be visible outside a module before, during and after the loading operation.

The Boot Loader shall provide an integrity check to ensure the integrity of the firmware and to ensure the integrity of any permanent security-critical data stored within a cryptographic module.

3.8 Physical Security

The Luna cryptographic module is a multi-chip stand-alone module as defined by FIPS PUB 140-2 section 4.5. The module is enclosed in a strong metal enclosure that provides tamper-response. Any tampering that might compromise a module's security is detectable by visual inspection of the tamper evident labels on the module. Refer to Section 3.10.1 Tamper Evident Labels for more information on the tamper evident labels.

Opening or removing the enclosure will cause a tamper signal and the module will respond as described below. 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.

The plaintext Critical Security Parameters (CSPs) stored inside the module are the Master Tamper Key (MTK), the Key Encryption Key (KEK) and the Token/Module Variable Key (TVK), which is used to implement the auto-activation feature. The MTK is stored in the battery-backed RAM in the security co- processor chip and the KEK and TVK are stored in the module's battery-backed RAM. The MTK and TVK are erased in the event of a tamper detection from the enclosure tamper signal. The KEK is erased when a decommission signal is received.

The module also senses and responds to out-of-range temperature and voltage conditions. In the event that the module senses an out-of-range temperature or voltage, it will clear all working memory and halt operations. It can be reset and placed back into operation when proper operating conditions have been restored.

3.8.1 Tamper Evident Labels

There are two tamper evident labels used on the module's enclosure: one covering a screw on the left side of the enclosure and one covering a screw on the rear side of the enclosure.

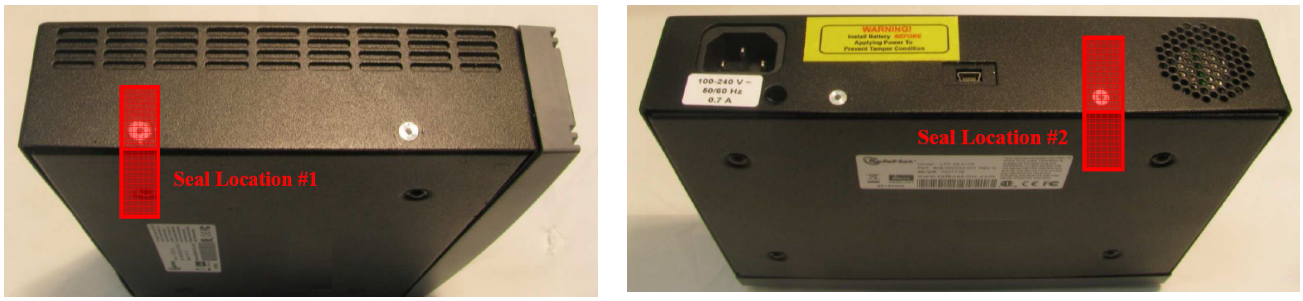


Figure 3-1. Tamper Evident Label Locations

Four variants of tamper evident labels have been evaluated for use with this module: TEL-GEMALTO, TEL-SAFENET, TEL-SAFENET-2, TEL-TRAC and TEL-TRAC-2. Any of these tamper evident labels can be used in the FIPS-validated configuration of the module. Refer to the photographs in Table 3-9 to identify the different tamper evident label variants.

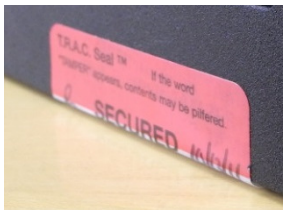
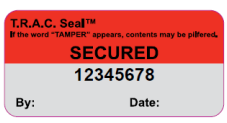
TEL-GEMALTO	TEL-SAFENET	TEL-SAFENET-2	TEL-TRAC	TEL-TRAC-2
				
				

Table 3-9. TEL-GEMALTO, TEL-SAFENET, TEL-SAFENET-2, TEL-TRAC and TEL-TRAC-2 Tamper Evident Labels

Tamper evident labels are applied to the module during the manufacturing process. The Security Officer should perform a visual inspection of the tamper evident labels for evidence of tamper.

3.9 EMI / EMC

The module conforms to FCC Part 15 Class B requirements for home use.

3.10 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 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.

3.11 Mitigation of Other Attacks

3.11.1 External Protection

The external metal enclosure of the G5 has a lid removal detection mechanism which, when triggered will cause a tamper event to be communicated to the cryptographic module. When the external tamper signal is asserted the NVRAM in the SafeXcel 3120 device is zeroized.

Timing attacks are mitigated directly by a module through the use of hardware accelerator chips, with built-in protection against such attacks, for crypto operations. The use of hardware acceleration ensures, for example, 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 further mitigate this type of attack.

3.11.2 Environmental Protection

While in operation the G5 will monitor the card input voltage, temperature, and battery state.

The G5 monitors input voltage to the CCA. The upper voltage limit is 12.7V. All on-board voltages are derived from the 12V input.

The G5 monitors the operating temperature of the assembly. Temperature excursions outside the 0 degrees Celsius to 60 degrees Celsius range are signaled as an exception to both the CPU and the SafeXcel 3120.

In the event that both power and the battery are removed, the G5 will zeroize the SafeXcel 3120 NVRAM.

4 User Guidance

4.1 FIPS-Approved Mode

The SO controls operation of a module in FIPS-approved mode, as defined by FIPS PUB 140-2, by enabling or disabling the appropriate Module Policy settings (assuming each is allowed at the Module Capability level). To operate in FIPS-approved mode, the following policy settings are required:

> "Non-FIPS Algorithms Available" must be disabled.

Additionally, for operation at FIPS Level 2:

> "Password authentication" must be enabled (implies that trusted path authentication is disallowed or disabled); and

> Raw RSA operations can only be used for key transport in FIPS mode

The policy setting for "Password authentication" may also be configured in the case where "Non-FIPS Algorithms Available" has been enabled.

If the SO selects policy options (i.e., enables "Non-FIPS Algorithms Available") that would place a module in a mode of operation that is not approved, a warning is displayed and the SO is prompted to confirm the selection. The SO can confirm that the cryptographic module is in FIPS mode by utilizing the "hsm showinfo" command. With this command, the following message will be displayed, "The HSM is in FIPS 140-2 approved operation mode". Operators are responsible for the following restrictions which will not be indicated by the "hsm showinfo" command.

> AES and Triple-DES key wrapping shall not be used. AES and Triple-DES key unwrapping is still allowed.

> In accordance to NIST guidance, operators are responsible for insuring that a single Triple-DES key shall not be used to encrypt more than 216 64-bit data blocks.

5 Security Policy Checklist Tables

Table 5-1. Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Security Officer	Identity-based	Level 2 - Password
Audit Officer	Identity-based	Level 2 - Password
Partition User	Identity-based	Level 2 - Password
Public User	Not required	N/A

Table 5-2. Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password (Level 2)	Configurable by SO from 7 to 16 characters. The probability of guessing the challenge secret in a single attempt is 1 in 62 (approximately 3.5 x 10). With login failure thresholds of 3 for SO and configurable from 1 to 10 (default 10) for users, this ensures the FIPS 140-2 required thresholds can never be reached.

All services listed in Table 5-3 can be accessed in FIPS and non-FIPS mode. The services listed in Table 5-3 use the security functions listed in Table 3-4, Table 3-5, and Table 3-6. When the module is operating in FIPS-approved mode as described in Section 4.1, the Non-FIPS Approved Security Functions in Table 3-6 are disabled and cannot be used for these services. The non-Approved functions in Table 3-7 can only be accessed through the services when the module is in non-FIPS Approved mode.

Table 5-3. Services Authorized for Roles

Role	Authorized Services
Security Officer	Show Status, Self-test, Initialize Module, Configure Module Policy, Create Partition, Configure Partition Policy, Zeroize, Firmware Update
Audit Officer	Show Status, Initialize and Configure Secure Audit Logging, Change Audit Officer's Password, Verify Secure Audit Log Files, Import and Export Secure Audit Log Files, Synchronize Module Clock with the Clock of the Host System, Import and Export the Wrapped Secure Audit Logging Key, Show Secure Audit Log Status.
Partition User	Show Status, Self-test, Key and Key Pair Generation, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Symmetric & Asymmetric Key Wrap/Unwrap, Symmetric & Asymmetric Key Mask/Unmask, Store Data Object, Read Data Object, Partition Backup and Restore
Public User	Show Status, Self-test, Store Public Data Object, Read Public Data Object

Table 5-4. Access Rights within Services

Service	Cryptographic Keys and CSPs	Role	Type(s) of Access
Show Status[5]	N/A	All	N/A
Self-test	N/A	SO and Partition User	N/A
Initialize Module	Authentication data via trusted path	SO	Write – SO authentication
Configure Module Policy	Authentication data via trusted path	SO	Use[6]
Create Partition	Authentication data via trusted path	SO	Write – User authentication
Configure Partition Policy	Authentication data via trusted path	SO	Use
Zeroize	Authentication data, symmetric keys, asymmetric key pairs	SO	Write, Erase
Firmware Update	MVK[7]	SO	Use, Write (firmware only)
Key and Key Pair	Symmetric keys, asymmetric key pairs	Partition User	Write
Symmetric Key Wrap/ Unwrap	Symmetric with RSA Symmetric with Symmetric ECB mode	Partition User	Use, Write
Asymmetric Key Wrap/	Asymmetric with Symmetric CBC mode	Partition User	Use, Write
Symmetric Key Mask/	Symmetric with AES 256	Partition User	Use, Write
Asymmetric Key Mask/	Symmetric with AES 256	Partition User	Use, Write
Partition Backup / Restore	Symmetric keys, asymmetric key pairs	Partition User	Transfer[8]
Symmetric Encrypt/Decrypt	Symmetric keys	Partition User,	Use
Asymmetric Signature	RSA, DSA private keys	Partition User,	Use
Asymmetric Verification	RSA, DSA public keys	Partition User,	Use
Store Data Object	Non-cryptographic data	Partition User, Public User[9]	Write
Read Data Object	Non-cryptographic data	Partition User, Public User[10]	Read
Initialize Secure Audit Logging	Symmetric keys	Audit Officer	Write
Change Audit Officer's	Authentication Data via trusted path	Audit Officer	Read, Write
Configure Secure Audit Logging	N/A	Audit Officer	Read, Write
Synchronize Module's clock with the Host	N/A	Audit Officer	Write

[5] Show status is provided by invoking the "hsm showinfo" command from the administrative interface. It will display identifying information about the module such as label, serial number, firmware version, etc., and state whether the module is in FIPS-approved mode.
[6] Use means access to key material for use in performing a cryptographic operation. The key material is never visible.
[7] Public key value. See Table 5-5 for its description.
[8] Transfer means moving a key using the cloning protocol from one cryptographic module to another.
[9] The Public User has access to Public Data Objects only.
[10] The Public User has access to Public Data Objects only.

Verify, Import, and Export secure audit log files	N/A	Audit Officer	Read
Show secure audit log	N/A	Audit Officer	Read
Import and Export the Wrapped Secure Audit	Symmetric keys	Audit Officer	Write, Read

Table 5-5. Keys and Critical Security Parameters

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Use
User Password	7-16 characters	N/A	Input in encrypted form	Flash memory in plaintext	Zeroized as part of a tamper event	Used in Password Authentication (Level 2) configuration only. The user provided password used for authentication in a Level 2 configuration. Minimum of 7 characters and maximum of 16.
Cloning Domain Vector	48-Byte value	Derived from password using concatenation KDF	Input via ICD interface	Flash memory encrypted with UGSK	N/A	48-byte value that is used to control a module's ability to participate in the cloning protocol. Encrypted with the USK / SMK.
User Storage Key (USK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted	N/A	The storage key for the user. This key is used to encrypt all sensitive attributes of all private objects owned by the user. Encrypted, as a part of the UAV, by the PIN key35.
Security Officer Master Key (SMK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted	N/A	The storage key for the SO. This key is used to encrypt all sensitive attributes of all private objects owned by the SO. Encrypted, as part of the SOV, by the PIN key.
Global Storage Key (GSK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted	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. Encrypted, as part of the UAV/SOV, by the PIN key
Secondary Global Storage Key (SGSK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with USKs and SMK	N/A	It is used to encrypt non-permanent parameters (parameters regenerated for every module initialization).
Token or Module Unwrapping Key (TUK)	RSA-2048 bit private key	ANSI X9.31	Not Input or Output	Flash memory encrypted with GSK	N/A	A 2048-bit RSA private key used in the cloning protocol.

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Use
Token or Module Wrapping Certificate (TWC)	RSA-2048 public / private certificate	Loaded at manufacturing	Public key output in plaintext	Flash memory plaintext	N/A	Used in exchange of session encryption key as part of the handshake during the cloning protocol.
U2 Key	3-Key Triple-DES	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with GSK	N/A	24-byte Triple-DES key used in conjunction with the auth code for a firmware update to derive a key used to decrypt the firmware update image when it is loaded into the module. Used for backwards compatibility purposes with earlier firmware versions.
Token or Module Variable Key (TVK)	AES-256	AES-CTR DRBG	Not Input or Output	Tamperable BBRAM in plaintext	Zeroized as part of a tamper event	Used to encrypt authentication data stored for auto- activation purposes. The non-volatile RAM is actively zeroized in response to a tamper event.
Master Tamper Key (MTK)	AES-256	AES-CTR DRBG	Not Input or Output	Tamperable BBRAM in plaintext	Zeroized as part of a tamper event	The MTK encrypts all sensitive values.
Key Encryption Key (KEK)	AES-256	AES-CTR DRBG	Output encrypted	Tamperable BBRAM in plaintext	Zeroized as part of a Decommission signal	The KEK encrypts all sensitive values and is zeroized in response to a decommission signal.
Masking Key	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted with SGSK	N/A	AES 256-bit key used during masking operations. Stored encrypted using the SGSK.
Manufacturer's Integrity Certificate (MIK)	RSA-4096 public key certificate	Loaded at manufacturing	Not Input or Output	Flash memory in plaintext	N/A	Used in verifying Hardware Origin Certificates (HOCs), which are generated in response to a customer function call to provide proof of hardware origin.
Manufacturer's Verification Key (MVK)	RSA-1024 public key	Loaded at manufacturing	Not Input or Output	Flash memory in plaintext	N/A	1024-bit public key counterpart to the Manufacturer's Signature Key (MSK) held at SafeNet. Used for key migration support for legacy HSMs
Device Authentication Key (DAK)	RSA 2048 bit private key			Flash memory encrypted with GSK		2048-bit RSA private key used for a specific PKI implementation requiring assurance that a key or a specific action

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Use
		ANSI X9.31	Not Input or Output		N/A	originated within the hardware crypto module.
Hardware Origin Key (HOK)	RSA 4096 bit private key	ANSI X9.31	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	Not Input or Output	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.
DRBG Key	AES-256	Hardware random source	Not Input or Output	Tamperable BBRAM in plaintext	Zeroized as part of a tamper event	32 bytes AES key stored in the BBRAM of the internal security co-processor. Used in the implementation of the NIST SP 800-90A CTR (AES) DRBG.
DRBG Seed	384 bits	Hardware random source	Not Input or Output	Tamperable BBRAM in plaintext	Zeroized as part of a tamper event	Random seed data drawn from the Hardware RBG in the security co-processor and used to seed the implementation of the NIST SP 800-90A CTR (AES) DRBG.
DRBG V	128 bits	Hardware random source	Not Input or Output	Tamperable BBRAM in plaintext	Zeroized as part of a tamper event	Part of the secret state of the approved DRBG. The value is stored in the security co-processor as plaintext and is generated using the methods described in SP800-90A.
DRBG Entropy Input	384 bits	Hardware random source	Not Input or Output	Tamperable BBRAM in plaintext	Zeroized as part of a tamper event	The entropy value used to initialize the approved DRBG. The 48-byte value is stored ephemerally in memory of the security co-processor.
Secure Audit Logging Key (SALK)	256 bit HMAC	AES-CTR DRBG	Input / Output encrypted	Flash memory in plaintext and encrypted with SADK	N/A	A 256-bit key used to verify the data integrity and the authentication of the log messages. It's saved in the parameter area of the Flash memory.

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Use
Secure Audit Domain Key (SADK)	AES-256	AES-CTR DRBG	Input / Output encrypted	Flash memory encrypted with USK	N/A	A 256-bit key that is used to wrap / unwrap the SALK when it is exported / imported from / to the module.