THALES
Building a future we can all trust

Thales Luna Backup Hardware Security Module

NON-PROPRIETARY SECURITY POLICY

Includes configurations Cloning [CL]

FIPS 140-2, Level 3

Document Information

Document Part Number	002-010965-001
Release Date	January 25, 2021

Revision History

Revision	Date	Reason
G	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.
H	January 25, 2021	Removed 186-2 Signature Generation and updated Tamper Label Picture.

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
SALK	Security Audit Logging Key

Term	Definition
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 deals only with operations and capabilities of the Thales Luna Backup 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 Backup 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-THALES and with Firmware Versions 6.24.6 or 6.24.7.

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

The Thales Luna Backup HSM is available in a cloning (CL) configuration.

The security policies described in this document apply to the Trusted Path Authentication (Level 3) configuration of the Thales Luna Backup 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 all level 3 requirements security requirements for FIPS 140-2, alongside the optional Environment Failure Protection (EFP) augmentation 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
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3

Security Requirements Section	Level
Mitigation of Other Attacks	3
Cryptographic Module Security Policy	3

2 Security Policy Model Introduction

2.1 Functional Overview

The Thales Luna Backup HSM is a 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 Backup HSM; Figure 2-2 depicts the Thales Luna Backup HSM cryptographic boundary.

The module may be purchased as either a FIPS Level 2 or FIPS Level 3 module. The end user can configure the modules to operate in either FIPS mode of operation or non-FIPS mode of operation. Configuration in FIPS mode of operation enforces the use of FIPS-approved algorithms only. For the FIPS Level 3 module the use of trusted path authentication is enforced. The module's FIPS mode can be changed by policy; changing this policy is destructive and will zeroize the module's non-volatile memory.

A cryptographic module is accessed directly (i.e., electrically) via either the Trusted Path PIN Entry Device (PED) serial interface or 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. 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 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 Backup HSM in a Trusted Path Authentication (FIPS Level 3) configuration.

Figure 2-1. Thales Luna Backup HSM

Figure 2-2. Thales Luna Backup 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
- 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 3.3.7, 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) or Partition Security Officer (PSO) 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 "enable domestic mechanisms & key sizes" 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 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 password authentication (disallowed in Trusted Path configuration);
- Allow/disallow trusted path authentication (allowed and must be enabled in Level 3 configuration);
- Allow/disallow masking;
- Allow/disallow cloning;
- Allow/disallow non-FIPS algorithms;
- Allow/disallow SO reset of partition PIN;
- Allow/disallow network replication;
- Allow/disallow remote authentication;
- Allow/disallow forcing change of User authentication data;
- Allow/disallow offboard storage;
- Allow/disallow partition groups;
- Allow/disallow Remote PED (RPED) operations;
- Allow/disallow external Master Tamper Key (MTK) split storage;
- Allow/disallow Acceleration;
- Allow/disallow unmasking;
- Allow/disallow FW5 compatibility mode;
- Maximum number of partitions;
- Allow/disallow ECIES support;
- Allow/disallow force single domain;

- Allow/disallow unified PED key;
- Allow/disallow M of N;
- Allow/disallow small form factor backup/restore;
- Allow/disallow Secure Trusted Channel;
- Allow/disallow decommission on tamper; and
- Allow/disallow partition re-initialize.

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 user key management capability. (This would be disabled by the SO/PSO at the policy level to prevent any key management activity in the partition, even by a user in the Crypto Officer role. This could be used, for example, at a CA once the root signing key pair has been generated and backed up, if appropriate, to lock down the partition for signing use only.);
- Allow/disallow incrementing of failed login attempt counter on failed challenge response validation (Ignore failed challenge responses);
- Allow/disallow activation;
- Allow/disallow automatic activation (auto-activation);
- Allow/disallow High Availability (HA) recovery;
- 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;
- Number of failed Partition User logins allowed before partitions is locked out/cleared. The default is 10 for user partition logins and Partition SO logins; SO/PSO can configure it to be 1<N>10. The default is 3 for SO logins; SO can configure it to be $1 \leq N \leq 3$.
- Minimum/maximum PIN length (configurable 7 to 255);
- Allow/disallow remote authentication;

- Allow/disallow RSA PKCS mechanism;
- Allow/disallow CBC-PAD (un)wrap keys of any size;
- Allow/disallow private key SFF backup/restore;
- Allow/disallow secret key SFF backup/restore; and
- Allow/disallow Force Secure Trusted Channel.

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[1];
- Allow/disallow secret key masking;
- Allow/disallow private key unmasking;
- Allow/disallow secret key unmasking;

The following tables summarize the module and partition capabilities, showing typical capability settings for Thales Luna Backup HSM's used in the following configurations (An X indicates the default capability setting for each configuration of the module.):

Thales Backup product configurations:

- Cloning (CL).

Table 3-1. Module Capabilities and Policies

Description	Capability	CL	Policy	Comments
Non-FIPS algorithms available	Allow	**X**	Enable	SO can configure the policy to enable or disable the availability of non-FIPS algorithms at the time the cryptographic module is initialized.
			Disable	
	Disallow		Disable	The cryptographic module must operate using FIPS-approved algorithms only. Must be disabled in FIPS mode
Password authentication	Allow		Enable	SO can configure the policy to enable or disable the use of passwords without trusted path for authentication.
			Disable	
	Disallow	**X**	Disable	The cryptographic module must operate using the trusted path and module-generated secrets for authentication.

[1] Key masking is a Thales product feature that provides encrypted key output. Key masking provides AES 256-bit encryption employing additional proprietary obfuscation, which does not provide additional security. Within the terms of FIPS 140-2 and supporting Implementation Guidance, this capability is a form of "key wrapping".

Description	Capability	CL	Policy	Comments
Trusted path authentication	Allow	X	Enable	The trusted path authentication is set by the Level 3 configuration to enable (true) and cannot be changed by the user.
			Disable	
	Disallow		Disable	The cryptographic module must operate using passwords without trusted path for authentication.[2]
Remote PED Operations	Allow	X	Enable	The cryptographic module can use Remote PED for Trusted Path authentication.[3] Allowed in Trusted Path authentication only.
			Disable	
	Disallow		Disable	The cryptographic module cannot use remote PED for Trusted Path authentication.
Cloning	Allow	X	Enable	SO can configure the policy to enable or disable the availability of the cloning function for the cryptographic module as a whole.
			Disable	
	Disallow		Disable	The cryptographic module must operate without cloning.
Masking	Allow		Enable	SO can configure the policy to enable or disable the availability of the masking function for the cryptographic module as a whole.
			Disable	
	Disallow	X	Disable	The cryptographic module must operate without masking.
Unmasking	Allow	X	Enable	SO can configure the policy to enable or disable the availability of the unmasking function for the cryptographic module as a whole.
			Disable	
	Disallow		Disable	The cryptographic module must operate without unmasking.
SO reset of partition PIN	Allow	X	Enable	SO can configure the policy to enable a partition PIN to be reset if it is locked as a result of exceeding the maximum number of failed login attempts.
			Disable	
	Disallow		Disable	A partition cannot reset the partition PIN and must be re-created as a result of exceeding the maximum number of failed login attempts.
Network Replication	Allow	X	Enable	

[2] One and only one means of authentication (“user password” or “trusted path”) must be enabled by the policy. Therefore, one of the authentication capabilities must be allowed and, if one of the capabilities is disallowed or the policy setting disabled, then the policy setting for the other must be enabled.

[3] Enabled in the Trusted Path configuration. Operator can connect the cryptographic module to a Remote PED using Command Line Interface (CLI) commands.

Description	Capability	CL	Policy	Comments
			Disable	SO can configure the policy to enable the replication of the module's key material over the network to a second module.
	Disallow		Disable	The module cannot be replicated over the network.
Force user PIN change	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If enabled, it forces the user to change the PIN upon first login.
			Disable	
	Disallow		Disable	The user is never forced to change PIN on first login.
Partition groups	Allow		Enable	This capability is set prior to shipment to the customer. It allows the use of partition groups.
			Disable	
	Disallow	**X**	Disable	Partition groups cannot be enabled for the module.
External MTK split storage	Allow	**X**	Enable	This capability is set prior to shipment to the customer. It allows the use of external storage of the MTK split.
			Disable	
	Disallow		Disable	External MTK split storage cannot be enabled for the module.
Acceleration	Allow	**X**	Enable	This capability is set prior to shipment to the customer. It allows the use of the onboard crypto accelerator.
			Disable	
	Disallow		Disable	Remote authentication cannot be enabled for the module.
FW5 compatibility mode	Allow		Enable	Allows the use of the FW5 compatibility mode. The compatibility mode allows the cryptographic module to use the legacy Token Wrapping Certificate (TWC) to communicate with the installed base of legacy units in the field.
			Disable	
	Disallow	**X**	Disallow	FW5 compatibility mode cannot be enabled for the module.
Maximum number of partitions	N	**X**	N	This capability is set prior to shipment to the customer. The default number of partitions allowed (N) is 1. For the three configurations shown here, the default is 20.
Remote Authentication	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If
			Disable	

Description	Capability	CL	Policy	Comments
				enabled it allows remote authentication.
	Disallow		Disallow	Remote Authentication cannot be enabled for the module.
Portable masking key (was Offboard Storage)	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If enabled it allows the use of the portable masking key (offboard storage).
			Disable	
	Disallow		Disallow	Use of the portable masking key (offboard storage) cannot be enabled for the module.
ECIES Support	Allow		Enable	This capability is set prior to shipment to the customer. If enabled it allows support for ECIES.
			Disable	
	Disallow	**X**	Disallow	ECIES support cannot be enabled for the module.
Force Single Domain	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If enabled it allows the forcing of a single domain for a module.
			Disable	
	Disallow		Disallow	The module cannot force a single domain.
Unified PED Key	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If enabled it allows the creation and use of a unified PED key.
			Disable	
	Disallow		Disallow	Unified PED key cannot be enabled for the module.
M of N	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If enabled it allows the use of M of N keys. If disabled, M and N are set to 1.
			Disable	
	Disallow		Disallow	M of N cannot be enabled for the module.
Small Form Factor Backup / Restore	Allow		Enable	This capability is set prior to shipment to the customer. If enabled it allows the use of small form factor backup and restore.
			Disable	
	Disallow	**X**	Disallow	Small form factor backup/restore cannot be enabled for the module.
Secure Trusted Channel	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If enabled it allows the use of the secure trusted channel.
			Disable	

Description	Capability	CL	Policy	Comments
	Disallow		Disallow	Secure trusted channel cannot be enabled for the module.
Decommission on Tamper	Allow		Enable	This capability is set prior to shipment to the customer. If enabled it allows decommission on tamper.
			Disable	
	Disallow	**X**	Disallow	Decommission on tamper cannot be enabled for the module.
Partition Re-initialize	Allow	**X**	Enable	This capability is set prior to shipment to the customer. If enabled it allows a partition to be re-initialized.
			Disable	
	Disallow		Disallow	Partition re-initialize cannot be enabled for the module.

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 (particularly for activation purposes, see section 3.3.2), plus the CA application running on a network-attached host computer.

3.2.2 Roles

In the Trusted Path Authentication configuration, the Thales cryptographic module supports the following authenticated operator roles: The Security Officer (SO) and Audit Officer at the module level, plus the Partition Security Officer (if applicable), Crypto Officer and Crypto User for each Partition. There is an additional Admin Partition in which the SO can optionally enable an authenticated Admin User role. The cryptographic module 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 Admin User is a privileged role which exists only for the Admin Partition, and is the key management role for the admin partition.

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, Crypto Officer, and Crypto 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 Security Officer is a privileged role, which exists only at the partition level to manage the partition policies and roles.

The Crypto Officer is the key management role for each partition and the Crypto User is an optional 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 Admin User, Audit Officer, Crypto Officer, Crypto User, Partition Security Officer or Security Officer role before identification and authentication;

> No identity can assume more than one authenticated role at the same time, e.g. Crypto Officer or Crypto User plus the Security Officer role, or Audit Officer plus Security Officer.

The CO can create the Crypto User role by creating a challenge value for the Crypto User. In the case of a partition that supports the Crypto Officer and Crypto User roles, the Security Officer can limit access to only the Crypto User role by disabling the “User Key Management” (see Table 3-1) policy.

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 (which can include both the Crypto Officer and Crypto User role per Partition) and SO/PSO account data:

> Partition ID;

> Partition encrypted authentication data (checkword);

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

> Partition locked flag.

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

> Only the Security Officer role can create 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 Partition SO can modify the following security attribute:

- Checkword for Partition SO

> 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, in the Crypto Officer or Crypto User role. 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 (Crypto Officer or Crypto User) associated with the user's login state, see section 3.3.7. 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, Partition SOs and the SO be authenticated by proving knowledge of a secret shared by the operator and the module. A module configured for Trusted Path Authentication must be initialized using the PED to define the SO authentication data.

For Trusted Path Authentication, a module generates the authentication secret as a 48-byte random value and, optionally for a Partition User, an authentication challenge secret. The authentication secret(s) are provided to the operator via a physically separate trusted path, described in sub-section 3.3.2, and must be entered by the operator via the trusted path and via a logically separate trusted channel (in the case of the response based on the challenge secret) during the login process. If a Partition is created with Crypto Officer and Crypto User roles, a separate challenge secret is generated for each role.

The following types of iKey are used with the Thales PED:

- Orange (RPV) iKey – for the storage of the Remote PED Vector (RPV);
- Blue (SO) iKey – for the storage of SO or Partition SO authentication data;
- Black (User) iKey – for the storage of User authentication data;

- Red (Domain) iKey – for the storage of the cloning domain data, used to control the ability to clone from a cryptographic module to a backup module;
- Purple (MTK Recovery) iKey – for the storage of an external split that allows the MTK to be restored after a tamper event; and
- White (Audit Officer) iKey – for the storage of Audit Officer authentication data.

Any iKey, 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.

3.3.2 Trusted Path

In Trusted Path mode, user authentication is, by default, a two-stage process. The first stage is termed "Activation" and is performed using a trusted path device (PED) which connects to the cryptographic module either directly over a physical wire or remotely over a secure network connection. The primary form of authentication data used during Activation is the 48-byte value that is randomly generated by a module and stored on the Black (User) iKey via the trusted path. The data on the iKey must then be entered into a module via the trusted path as part of each Activation process. Once Activation has been performed, the user's Partition data is ready for use within a module. Access to key material and cryptographic services, however, is not allowed until the second stage of authentication, "User Login", has been performed. This typically requires the input of a partition's challenge secret as part of a login operation. However, for SO authentication, Partition SO authentication and for user authentication when the settings of the Partition Policy disable the use of challenge/response authentication for login to a partition, the presentation of the iKey data (i.e., equivalent to Activation) is all that is required to complete authentication.

The default Partition Policy enables the use of challenge/response authentication for the "User Login" stage. The authentication challenge secret (or secrets if the Crypto Officer and Crypto User roles are used) for the partition is generated by the module as a 75-bit value that is displayed as a 16 character alphanumeric string on the visual display of the trusted path device. The challenge secret is then provided, via a secure out-of-band means, to each external entity authorized to connect to the partition and is used by the external entity to form the response to a random one-time challenge from a module. The encrypted one-time response is returned to the cryptographic module where it is verified to confirm the "User Login". Thus, when the challenge secret is required, both the trusted path Activation and the successful completion of the challenge/response process by the external entity is required to authenticate to a partition and have access to its cryptographic material and functions.

3.3.3 Remote PED Operation

The user has the option of operating the PED in the conventional manner (i.e., locally connected to the cryptographic module) or remotely, connected to a management workstation via USB. Remote PED operation extends the physical trusted path connection by the use of a protocol 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 iKeys are performed in exactly the same way as they would be when locally connected.

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

At the time it is initialized, the module generates a random 256-bit secret, known as the Remote PED Vector (RPV), stores it in its secure parameters area, and writes it to the “Orange” iKey, also known as the Remote PED Key (RPK).

To establish the secure connection, the RPK must be inserted into the PED. The PED extracts the RPV, and the 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.

3.3.4 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 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.

3.3.5 M of N Authentication

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

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

When the M of N set is distributed to recipients outside the module, the split data is contained in M of N vectors. A vector may contain one or more splits depending on the weight assigned at the time of generation. For example, in the case of a three-of-five activation setting, it may be desired for A to receive the equivalent of two splits whereas B, C and D only receive one each for a total of five.

3.3.6 Limits on Login Failures

The module also implements a maximum login attempts policy. The policy differs for an SO authentication data search, a Partition 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 ”m” consecutive SO logon attempts fail, a module is zeroized. “m” is set at the time the cryptographic module is initialized, and can be modified by the SO. The valid range is 1-3.

In the case of a Partition SO authentication data search:

> If “p” consecutive Partition SO logon attempts fail, the partition is zeroized. “p” is set at the time the partition is initialized and can be modified by the PSO. The valid range is 1-10.

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

> If “SO reset of partition PIN” is Allowed and Enabled, then if “n” consecutive operator logon attempts fail, the module locks the Partition User. “n” is set at the time the partition is initialized and can be modified by the SO/PSO. The valid range is 1-10. The SO/PSO must unlock the partition in order for the Partition User to resume operation.

> If “SO reset of partition PIN” is not Allowed or not Enabled, then if “n” consecutive Partition User logon attempts fail, the module will erase/zeroize the partition. The SO/PSO must re-create/initialize 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.

3.3.7 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[4].** If True, object may be extracted. If False, object may not be extracted.
- **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

[4] 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.

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 3-2 summarizes the object attributes used in Access Control Policy enforcement.

Table 3-2. 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.
	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 following constraints:
  - A Partition User in the Crypto User role has access to only the User operations; and

- The restrictions imposed by the cryptographic module and Partition Capability and Policy settings.

3.3.8 Object Protection

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

> User Storage Key (USK) – this key is created when the User, PSO or SO is created/initialized. It is used to encrypt all sensitive attributes of all private objects owned by the User/PSO/SO.

> Partition Storage Key (PSK) – this key is created by the cryptographic module when a partition is created/initialized. It is unique per-partition and is used to encrypt all CSP that are shared by all roles of a given partition.

> 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.

3.3.9 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.

3.3.10 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 policies;

> Configuring the partition policies for partitions without a Partition SO role; and

> Firmware update.

The module shall restrict the performance of the following functions to the Partition SO role for a partition only:

> Configuring the partition policies for the partition with the Partition SO role.

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 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; and
- Key Derivation in accordance with NIST SP 800-108 (Counter mode).

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.

> 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). Symmetric key wrapping is supported via SP 800-38F AES key wrap mode.

> 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, see Section 3.5.1) 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 Thales 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 Thales cryptographic module's general secret key until such time as its memory locations (flash or RAM) are re-allocated for additional data on a Thales cryptographic module, at which time they are purged and zeroized before re-allocation.
- Objects on a Thales 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 Thales cryptographic module are zeroized.

- Objects on a Thales cryptographic module that are destroyed through C_InitToken (the SO-accessible command to initialize a Thales 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 Thales product feature that uses a one-time, 256-bit AES key as a session key to encrypt an object being transferred from one Thales 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.

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 (KTS) 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 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-1, SHA-224, SHA-256, SHA-384, SHA-512, RSA 2048-3072 bits (PSS) with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RSA 2048-3072 bits (ANSI X9.31) with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512; DSA 2048-3072 bits with SHA-224, SHA-256, SHA-384 and SHA-512; 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, SHA-384 and SHA-512; 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;
- Hash generation SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 180-4);
- Keyed hash generation HMAC using SHA-1[5], 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); and
- Deterministic Random Bit Generation (DRBG) (NIST SP 800-90A section 10.2.1)

Table 3-3. Approved Security Functions for SafeXcel 3120

Approved Security Functions	Certificate No.
Symmetric Encryption/Decryption	
AES: (ECB, CBC, GCM[6]); Encrypt/Decrypt; Key Size = 128, 192, 256)	#4849
Triple-DES: (ECB, CBC); Encrypt/Decrypt KO 1)	#2552
Hashing	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	#3988

[5] Only keys of 112 bits or greater are allowed in FIPS mode when using HMAC-SHA-1.
[6] The module generates IVs internally using the Approved DRBG which are at least 96-bits in length.

Approved Security Functions	Certificate No.
Message Authentication Code	
HMAC-SHA-1[7], HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	#3306
Triple-DES MAC (based on Certificate No. #2552)	Vendor Affirmed
Asymmetric	
RSA: FIPS186-2: Signature Verification FIPS186-4: Key Generation, Signature Generation, Signature Verification	#2691
DSA: FIPS186-4: PQG Generation, Key Generation, Signature Generation, Signature Verification	#1298
ECDSA: FIPS186-4: Key Generation, Signature Generation, Signature Verification	#1242
Random Number Generation	
NIST SP 800-90A DRBG (CTR) AES-256	#1704

Table 3-4. Approved Security Functions for Firmware Implementation

Approved Security Functions	Certificate No.
Symmetric Encryption/Decryption	
AES: (ECB, CBC, OFB, CFB8, CFB128, CTR, GCM[6], KW)	#5012
Triple-DES: (ECB, CBC, OFB, CFB8, CFB64, CTR)	#2585
Hashing	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	#4075
Message Authentication Code	
HMAC-SHA-1[8], HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	#3330
Triple-DES MAC (based on Certificate No. #2585)	Vendor Affirmed
Triple-DES CMAC	#2585
AES CMAC (Key Sizes Tested: 128, 192, 256)	#5012
Asymmetric	
RSA: FIPS186-2: Signature Verification FIPS186-4: Key Generation, Signature Generation, Signature Verification	#2704
DSA:	#1315

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

Approved Security Functions	Certificate No.
FIPS186-4: PQG Generation, Key Generation, Signature Generation, Signature Verification	
ECDSA: FIPS186-4: Key Generation, Signature Generation, Signature Verification	#1278
CVL: FIPS186-4: Signature Generation Component	#1562
Key Agreement Scheme	
ECC: Ephemeral Unified (KARole(s): Initiator / Responder) OnePassDH (KARole(s): Initiator / Responder)	#154
Key Derivation	
NIST SP 800-108 (Counter Mode)	#164
Key Transport	
KTS (AES Cert. #5012; key establishment methodology provides between 128 and 256 bits of encryption strength)	#5012

Table 3-5. 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)	
EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 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)	
Entropy Source	
Hardware Random Number Generator (free-running local oscillators)	

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 3-6. Non-FIPS Approved Security Functions

Non-FIPS Approved Security Functions
Symmetric Encryption/Decryption

DES
Triple-DES (2-Key)
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[9]
SSL3-SHA1-MAC[10]
HMAC (Certs. #3306 and #3330 – non-compliant less than 112 bits of encryption strength)
Asymmetric
KCDSA
RSA X-509
RSA (Certs. #2691 and #2704 – non compliant less than 112 bits of encryption strength)
DSA (Certs. #1298 and #1315 – non-compliant less than 112 bits of encryption strength)
ECDSA (Certs. #1242 and #1278 – non-compliant less than 112 bits of encryption strength)
Generate Key
DES
RC2
RC4

[9] Used by the TLS protocol. TLS has not been reviewed or tested by the CAVP or the CMVP.
[10] Used by the TLS protocol. TLS has not been reviewed or tested by the CAVP or the CMVP.

RC5
CAST5
SEED
ARIA
GENERIC-SECRET
SSL PRE-MASTER[11]
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)

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. The module also performs conditional self-tests in accordance with FIPS 140-2, section 4.9.2.

Table 3-7. 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[12]
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[13]
SHA-1 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
SHA-224 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt

[11] Used by the TLS protocol. TLS has not been reviewed or tested by the CAVP or the CMVP.
[12] Details of the failure can be obtained from the dual-port following a module halt.
[13] An error message is output, the cryptographic module halts, and data output is inhibited.

Test	When Performed	Where Performed	Indicator
SHA-256 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
SHA-384 KAT	Power-on/Request	Firmware / Hardware	Module halt / Error - Halt
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

Test	When Performed	Where Performed	Indicator
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
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 Thales Hardware Security Module is a multi-chip standalone 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 Security Officer should perform a visual inspection of the module at regular intervals. If physical tamper is discovered, the Security Officer should remove the module from service and follow corporate security guidelines. 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, KEK and TVK are stored in battery-backed

RAM. The MTK and TVK are erased in the event of a tamper detection – either from the external tamper signal or from removal of the card from the PCI-Express slot. The KEK is erased when a decommission signal is received.

The module is designed to operate between 0° and 65° Celsius, and to sense and respond to out-of-range temperature conditions. The module also senses and responds to out-of-range 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.

The epoxy hardness was tested at room temperature and at the high and low temperatures which would cause the active tamper (0° to 65° Celsius).

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-THALES. Any of these tamper evident labels can be used in the FIPS-validated configuration of the module. Refer to the photographs in Table 3-8 to identify the different tamper evident label variants.

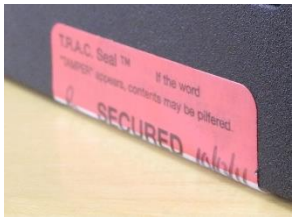
TEL-GEMALTO	TEL-SAFENET	TEL-SAFENET-2	TEL-TRAC	TEL-TRAC-THALES
				
				

Table 3-8. TEL-GEMALTO, TEL-SAFENET, TEL-SAFENET-2, TEL-TRAC and TEL-TRAC-THALES 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.

3.8.2 Secure Recovery

When the MTK is created, two splits are also created – one split is held within the battery-backed RAM and the other is passed to the module firmware. The module's split can then be written out to iKey (Purple Key) tokens, using the M of N feature. These iKeys are known as Secure Recovery Keys (SRKs). If a tamper event occurs, it is possible to return the module to operation, after ensuring the tamper condition has been cleared, by recovering the MTK from the internal split and the value(s) stored on the external SRK iKey token(s). The Secure Recovery feature can also be used to enable secure shipment of the module. This is done by invoking a cryptographic module command that deliberately erases the MTK and flags the operation as being a "secure transport" operation, rather than an actual tamper event. This ensures that the module's sensitive objects are cryptographically protected and the module cannot be used in a malicious fashion while it is en route to its destination. At the receiving site, the module can be put into operation using the Secure Recovery feature.

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

Timing attacks are mitigated directly by a 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.

The cryptographic module provides a connection to allow it to receive an external tamper event signal. By responding to the signal a module can ensure that no sensitive data remain even if a determined attack defeats the external physical security protection measures. There are two sources for a potential tamper signal. The first is circuitry to detect the removal of a module from a PCI-Express slot. By responding to this external signal, the module ensures that all plaintext sensitive data are cleared if a module is removed from its slot. The second source is used only in the instance of an appliance installation. In that case, the signal would come from tamper detection circuitry that detects opening of the appliance cover. By responding to this external signal, the module ensures that all plaintext sensitive data are cleared if the appliance cover is opened.

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 3:

> "Trusted path authentication" must be enabled (implies that password authentication is disallowed or disabled);

> "Count failed challenge – response validations" must be enabled if activation or auto-activation is enabled; and

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

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, "This HSM is 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 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 3 – Authentication token (PED Key – one per module) plus optional PED PIN
Admin User	Identity-based	Level 3 – Authentication token (PED Key – one per module) plus optional PED PIN
Audit Officer	Identity-based	Level 3 – Authentication token (PED Key – one per module) plus optional PED PIN
Partition Security Officer	Identity-based	Level 3 – Authentication token (PED Key – one per partition with a PSO) plus optional PED PIN
Crypto Officer	Identity-based[14]	Level 3 – Authentication token (PED Key – one per user) plus optional PED PIN, plus optional Challenge Secret for the role[15]
Crypto User	Identity-based	Level 3 – Authentication token (PED Key – one per user) plus optional PED PIN, plus optional Challenge Secret for the role
Public User	Not required	N/A

Table 5-2. Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
PED Key (Level 3) plus PIN	48-byte random authentication data stored on PED key plus PIN entered via PED keypad (minimum 4 bytes). It is obvious that the probability of guessing the authentication data in a single attempt is 1 in 2^{384}. With login failure thresholds of 1 to 3 for SO and configurable from 1 to 10 (default 10) for partition SOs and users, this ensures the FIPS 140-2 required thresholds can never be reached.
Challenge Secret (Level 3)	Default 16 character random string (minimum 7 character string). The probability of guessing the challenge secret in a single attempt is 1 in 62^7 (approximately 3.5×10^{12}). With login failure thresholds of 1 to 3for SO and configurable from 1 to 10 (default 10) for partition SOs and users, this ensures the FIPS 140-2 required thresholds can never be reached.

[14] The Crypto Officer and Crypto User both apply to the same partition, i.e., identity. They are distinguished by different challenge values representing the two different roles.
[15] If activation or auto-activation is enabled, challenge secret is required in FIPS mode.

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 3-3, Table 3-4, and Table 3-5. When the module is operating in FIPS-approved mode as described in Section 4.1, the Non-FIPS Approved Security Functions in Table 3-5 are disabled and cannot be used for these services. The non-Approved functions in Table 3-6 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, Initialize Partition, Configure Partition Policy, Initialize Role, Reset Role Authentication Data, Change Role Authentication Data,, Zeroize Module, Zeroize Partition, Delete Partition, Firmware Update, Configuration Update, Generate Random Data, Key Generation, Key Pair Generation, Symmetric Key Wrap/Unwrap, Asymmetric Key Unwrap, Symmetric Key Mask/Unmask, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Store Data Object, Read Data Object, Partition Backup and Restore
Admin User	Show Status, Self-test, Change Role Authentication Data, Zeroize Module, Zeroize Partition, Generate Random Data, , Key Pair Generation, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Symmetric Key Wrap/Unwrap, Asymmetric Key Wrap/Unwrap, Symmetric & Asymmetric Key Mask/Unmask, Store Data Object, Read Data Object
Audit Officer	Show Status, Self-test, Change Role Authentication Data, Zeroize Module, Zeroize Partition, Generate Random Data, 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 Security Officer	Show Status, Self-test, Initialize Partition, Configure Partition Policy, Initialize Role, Reset Role Authentication Data, Change Role Authentication Data, Zeroize Module, Zeroize Partition, Generate Random Data
Crypto Officer	Show Status, Self-test, Initialize Role, Reset Role Authentication Data, Change Role Authentication Data, Zeroize Module, Zeroize Partition, Generate Random Data, Key Generation, Key Pair Generation, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Symmetric Key Wrap/Unwrap, Asymmetric Key Wrap/Unwrap, Symmetric & Asymmetric Key Mask/Unmask, Store Data Object, Read Data Object, Partition Backup and Restore
Crypto User	Show Status, Self-test, Change Role Authentication Data, Zeroize Module, Zeroize Partition, Generate Random Data, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Store Data Object, Read Data Object
Public User	Show Status, Self-test, Zeroize Module, Zeroize Partition, 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[16]	N/A	All	N/A
Self-test	N/A	All	N/A
Initialize Module	Authentication data via trusted path	SO	Write – SO authentication data
Configure Module Policy	Authentication data via trusted path	SO	Use[17]
Create Partition	Authentication data via trusted path	SO	Write – User authentication data
Initialize Partition	Authentication data via trusted path	SO, PSO	Write – PSO authentication data
Configure Partition Policy	Authentication data via trusted path	SO, PSO	Use
Initialize Role	Authentication data via trusted path	SO, PSO, Crypto Officer	Write – User/PSO authentication data
Reset Role Authentication Data	Authentication data via trusted path	SO, PSO, Crypto Officer	Write – User/PSO authentication data
Change Role Authentication Data	Authentication data via trusted path	SO, PSO, Crypto Officer, Crypto User, Audit Officer, Admin User	Use, Write – User/PSO authentication data
Zeroize Module	N/A	All	Erase
Zeroize Partition	N/A	All	Erase
Delete Partition	Authentication data via trusted path	SO	Erase
Firmware Update	MVK[18]	SO	Use, Write (firmware only)
Configuration Update	Authentication data via trusted path	SO	Use, Erase
Generate Random data	N/A	SO, PSO, Crypto Officer, Crypto User, Audit Officer, Admin User	Use
Key Generation	Symmetric keys	SO, Crypto Officer, Admin User	Write

[16] Show status is provided by invoking the “hsm show” command from the administrative interface. It will display identifying information about the module such as label, serial number, firmware version, etc. The “hsm capability list” command indicates whether the module is in FIPS-approved mode.
[17] Use means access to key material for use in performing a cryptographic operation. The key material is never visible.
[18] Public key value. See Table 5-5 for its description.

Service	Cryptographic Keys and CSPs	Role	Type(s) of Access
Key Pair Generation	Asymmetric key pairs	SO, Crypto Officer, Admin User	Write
Symmetric Key Wrap / Unwrap	Symmetric with RSA Symmetric with Symmetric Key Wrap mode[19]	SO, Crypto Officer, Admin User	Use, Write
Asymmetric Key Wrap / Unwrap	Asymmetric with Symmetric Key Wrap mode[20]	SO, Crypto Officer, Admin User	Use, Write
Symmetric Key Mask / Unmask	Symmetric with AES 256	SO, Crypto Officer, Admin User	Use, Write
Asymmetric Key Mask / Unmask	Symmetric with AES 256	SO, Crypto Officer, Admin User	Use, Write
Partition Backup / Restore	Symmetric keys, asymmetric key pairs	SO, Crypto Officer	Transfer[21]
Symmetric Encrypt / Decrypt	Symmetric keys	SO, Crypto Officer, Crypto User, Admin User	Use
Asymmetric Signature	RSA, DSA private keys	SO, Crypto Officer, Crypto User, Admin User	Use
Asymmetric Verification	RSA, DSA public keys	SO, Crypto Officer, Crypto User, Admin User	Use
Store Data Object	Non-cryptographic data	SO, Crypto Officer, Crypto User, Public User[22], Admin User	Write
Read Data Object	Non-cryptographic data	SO, Crypto Officer, Crypto User, Public User[23], Admin User	Read
Initialize Secure Audit Logging	Symmetric keys	Audit Officer	Write

[19] That is, the keys used during Symmetric Key Wrap/ Unwrap operations are a symmetric key wrapping key and the (symmetric or asymmetric) key which is being wrapped.
[20] That is, the keys used during Asymmetric Key Wrap / Unwrap operations are an asymmetric key wrapping key and the symmetric key which is being wrapped.
[21] Transfer means moving a key using the cloning protocol from one cryptographic module to another.
[22] The Public User has access to Public Data Objects only.
[23] The Public User has access to Public Data Objects only.

Service	Cryptographic Keys and CSPs	Role	Type(s) of Access
Change Audit Officer's Password	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 system's clock	N/A	Audit Officer	Write
Verify, Import, and Export secure audit log files	N/A	Audit Officer	Read
Show secure audit log status	N/A	Audit Officer	Read
Import and Export the Wrapped Secure Audit Logging Key	Symmetric keys	Audit Officer	Write, Read

Table 5-5. Keys and Critical Security Parameters

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Description
Challenge Secret	16 character data string	AES-CTR DRBG	Output via direct connection to PED	Flash memory encrypted with PSK	N/A	Used in Trusted Path Authentication configuration only. 16 character random string generated by the cryptographic module and output via the PED display when the user is created. It is input by the operator as the authentication data for a client application login.
Random Challenge	One-time random number	AES-CTR DRBG	Output to host using ICD communication path	Working RAM in plaintext	Power Cycle	Used in Trusted Path Authentication configuration only. A one-time random number generated by the cryptographic module and sent to the calling application for each login. It is combined with the input Challenge Secret to compute the one-time response that is returned to the cryptographic module.
Challenge Response	20-byte value	N/A	Input from host using ICD communication path	Working RAM in plaintext	Power Cycle	A 20-byte value used for authentication in the challenge response scheme. It is generated using the challenge secret and the one-time random challenge value.
PED[24] Key (or iKey) Authentication Data	48-byte random value	AES-CTR DRBG	Input / Output via direct connection to PED	Flash memory encrypted	N/A	Used in Trusted Path Authentication configuration. A 48-byte random value that is generated by the module when the SO or User is created. It is

[24] Within this document the terms “PED” key and “iKey” are interchangeable unless otherwise indicated.

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Description
						written out to the serial memory device (PED key) via the Trusted Path.
Optional PIN	PIN	N/A	Input on the PED via secure channel. PED does not input or output the PIN.	Not stored On module	N/A	An optional PIN value used for authentication along with the PED key. It must be a minimum of 4-bytes long
Cloning Domain Vector	48-Byte value	AES-CTR DRBG	Output via direct connection to PED	Flash Memory encrypted with PSK	N/A	48-byte value that is used to control a module's ability to participate in the cloning protocol. It is either generated by the module or imprinted onto the module at the time the module is initialized. The value is output from the original module in the domain onto a PED key to enable initializing additional modules into the same domain.
User Storage Key (USK)	AES-256	AES-CTR DRBG	Not Input or Output	Flash memory encrypted	N/A	This key is used to encrypt all sensitive attributes of all private objects owned by the user. Encrypted, as part of the partition data, by the key taken from the PED key data.
Partition Storage Key (PSK)	AES-256	AES-CTR-DRBG	Not Input or Output	Flash memory encrypted	N/A	The storage key for the SO/user partition. This key is used to encrypt the key data for the SO/user partitions. Encrypted as part of the SO/user partition data by the SO/user storage key (USK).
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 Thales cryptographic module. It is used

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Description
						to encrypt permanent parameters within the non-volatile memory area reserved for use by the module. Encrypted, as part of the partition data, by the SO/User partition storage key (PSK).
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.
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	It is 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

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Description
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 PSK	N/A	AES 256-bit key used during masking operations. Stored encrypted using the PSK.
Manufacturer's Integrity Certificate (MIC)	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 Thales. Used for key migration support for legacy HSMs.
Device Authentication Key (DAK)	RSA 2048 bit private key	ANSI X9.31	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 Certificate (DAC)	RSA 2048 public key certificate	Loaded at manufacturing	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.
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.

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Description
						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.
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.
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.509public key certificate corresponding to the ECC DAK. It is signed by the ECC HOK.

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Description
Remote PED Vector (RPV)	256-bit secret value	AES-CTR DRBG	Input / Output via direct connection to PED	Flash memory in plaintext	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.
Secure Recovery Vector (SRV)	Split of AES-256 MTK	AES-CTR DRBG	Split output in plaintext	Flash memory encrypted with GSK	N/A	A split of the MTK that is written to one or more iKeys using the M of N secret splitting scheme and used to recover the MTK after a tamper event has been cleared.
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	H/W 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 NIST SP 800-90A.
DRBG Entropy Input	384 bits	H/W 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.

Keys and CSPs	CSP Type	Generation	Input / Output	Storage	Destruction	Description
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 data integrity and authentication of the log messages. Saved in the parameter area of Flash memory.
Secure Audit Domain Key (SADK)	AES-256 KW	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.
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.