LEVEL 2 SECURITY POLICY FOR

Luna® PCM Cryptographic Module (includes configurations Key Export – SIM; Key Export – Cloning; Signing; and Signing-Backup)

DOCUMENT NUMBER:	CR-2372
AUTHOR:	Terry Fletcher
DEPARTMENT:	Engineering
LOCATION OF ISSUE:	Ottawa
DATE ORIGINATED:	March 16, 2006
REVISION LEVEL:	8
REVISION DATE:	August 9, 2007
SUPERSESSION DATA:	CR-2372, Revision 7
SECURITY LEVEL:	

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

1. INTRODUCTION

1.1. Purpose

This document describes the security policies enforced by SafeNet Canada Inc.'s Luna® PCM Cryptographic Module, also known as the G4.

This document applies to Hardware Versions LTK-02-0301 and LTK-02-0501, Firmware Version 4.6.1

1.2. Scope

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

2. SECURITY POLICY MODEL INTRODUCTION

2.1. Functional Overview

The Luna PCM cryptographic module is a multi-chip standalone hardware cryptographic module in the form of a PCMCIA card that typically resides within a custom computing or secure communications appliance. It is contained in its own secure enclosure that provides physical resistance to tampering. The cryptographic boundary of the module is defined to encompass all components inside the secure enclosure on the PCM card. Figure 2-1 depicts the Luna PCM cryptographic module.

The Luna PCM may be explicitly configured to operate in FIPS Level 2 mode, or in a non-FIPS mode of operation. Configuration in FIPS mode enforces the use of FIPS-approved algorithms only.

The cryptographic module is accessed directly (i.e., electrically) via the PCMCIA communications interface. The module provides secure key generation and storage for symmetric keys and asymmetric key pairs along with symmetric and asymmetric cryptographic services. Access to key material and cryptographic services for users and user application software is provided indirectly through the host appliance. It provides the ability to manage multiple user definitions and concurrent authentication states. The software on the host that provides the connections to the module presents a logical view of "virtual tokens" or "partitions" 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 Luna PCM in a **Password Authentication (FIPS Level 2)** configuration.

Figure 2-1. Luna PCM Cryptographic Module

2.2. Assets to be Protected

The module is designed to protect the following assets:

1. User-generated private keys,
2. User-generated secret keys,
3. Cryptographic services, and
4. Module security critical parameters.

2.3. Operating Environment

The module is assumed to operate as a key management and cryptographic processing card connected to a host computer via a peripheral interface and card reader. The host computer will normally be used in an internal network environment when key management security is a primary requirement. It is assumed that the host computer runs a suitably secured operating system, with only known versions of the permitted application services running on it.

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

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

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.

The Identification and Authentication policy is crucial for security enforcement and it is described in section 3.4. The access control policy is the main security functional policy enforced by the module and is described in section 3.5, which also describes the supporting object re-use policy. Cryptographic Material Management is described in section 3.6. Firmware security, physical security and fault tolerance are described in sections 3.8 through 3.11.

3.1. Operational Policy

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

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

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

3.1.1. Module Capabilities

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

- Allow/disallow non-FIPS algorithms available.
- Allow/disallow password authentication. (Allowed in Level 2 configuration)
- Allow/disallow trusted path authentication. (Disallowed in Level 2 configuration)
- Allow/disallow M of N. (Disallowed in Level 2 configuration)
- Allow/disallow cloning.
- Allow/disallow masking.
- Allow/disallow off-board storage.
- Allow/disallow M of N auto-activation. (Disallowed in Level 2 configuration)
- Allow/disallow ECC mechanisms.
- Number of failed SO logins allowed before the Hardware Security Module (HSM) is zeroized (set to 3).
- Allow/disallow Korean Digital Signature algorithms.
- Allow/disallow Remote Authentication. (Not applicable)
- Allow/disallow SO reset of partition PIN.
- Allow/disallow network replication.
- Allow/disallow forcing PIN change.

3.1.2. 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 zero) equates to disallow the functionality and true (or one) equates to allow the functionality. The remainder of the elements are integer values of the indicated number of bits.

- Allow/disallow partition reset.
- Allow/disallow activation.
- Allow/disallow automatic activation.
- Allow/disallow High Availability (HA).
- Allow/disallow multipurpose keys.
- Allow/disallow changing of certain key attributes once a key has been created.
- 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 Level 3 operation without a challenge. (Not applicable)
- Allow/disallow user key management capability. (Not applicable)
- Allow/disallow incrementing of failed login attempt counter on failed challenge response validation.
- Allow/disallow RSA signing without confirmation
- Allow/disallow Registration Authority (RA) type wrapping.
- Minimum/maximum password length (minimum must be >= 7).
- Number of failed Partition User logins allowed before partition is locked out/cleared. (The maximum value, set as the default, is 10.)

The following capabilities are only configurable if cloning is allowed and enabled at the module level:

- Allow/disallow private key cloning.
- Allow/disallow secret key cloning.

The following capabilities are only configurable if masking is allowed and enabled at the module level:

- Allow/disallow private key masking.
- Allow/disallow secret key masking.

In addition, the masking function can only be used according to the following restrictions:

- If cloning is not allowed or not enabled, masking/unmasking can only be used by the original module within its host appliance.
- If cloning is allowed and enabled, masking/unmasking can be used across multiple modules within the same domain.

The following tables summarize the module and partition capabilities, showing the typical capability settings for modules configured as Luna PCM Signing (S), Signing with Backup (SB), Key Export – Cloning (KEC) and Key Export – SIM (KES) modules. An **X** indicates the default capability setting for each configuration of the module. Greyed-out rows indicate that the corresponding capability setting is not used as a default for any of the configurations of the module.

Table 3-1 Module Capabilities and Policies

Description	Capability	S	SB	KEC	KES	Policy	Comments
Non-FIPS algorithms available	Allow	X	X	X	X	Enable Disable	SO can configure the policy to enable or disable the availability of non-FIPS algorithms at the time the HSM is initialized.
	Disallow					Disable	The HSM must operate using FIPS-approved algorithms only. Must be disabled in FIPS mode
Password authentication	Allow	X	X	X	X	Enable Disable	SO can configure the policy to enable or disable the use of passwords without trusted path for authentication.
	Disallow					Disable	The HSM must operate using the trusted path and module-generated secrets for authentication.
Trusted path authentication	Allow					Enable Disable	SO can configure the policy to enable or disable the use of the trusted path and module-generated secrets for authentication.
	Disallow	X	X	X	X	Disable	The HSM must operate using passwords without trusted path for authentication.[1]
M of N	Allow					Enable Disable	SO can configure the policy to enable or disable the use of M of N secret sharing to activate the module. Requires that the policy for "trusted path" authentication be enabled.
	Disallow	X	X	X	X	Disable	The HSM must operate without M of N secret sharing for activation.
Cloning	Allow		X	X	X	Enable Disable	SO can configure the policy to enable or disable the availability of the cloning function for the HSM as a whole.
	Disallow	X				Disable	The HSM must operate without cloning.
Masking	Allow		X		X	Enable Disable	SO can configure the policy to enable or disable the availability of the masking function for the HSM as a whole.
	Disallow	X		X		Disable	The HSM must operate without masking.
Off-board Storage	Allow		X	X	X	Enable Disable	Off-board storage is used for backup purposes in the Luna PCM stand-alone configuration. The SO can enable or disable the use of off-board storage.
	Disallow	X				Disable	Off-board storage is not allowed in the PCM configuration.
M of N auto-activation	Allow					Enable Disable	SO can configure the policy to enable or disable the use of the M of N auto-activation feature.
	Disallow	X	X	X	X	Disable	The HSM must operate without M of N auto-activation.
ECC mechanisms available	Allow	X	X	X	X	Enable Disable	This capability is set prior to shipment to the customer. It controls the availability of ECC mechanisms.
	Disallow					Disable	ECC mechanisms are not available.
Partition reset	Allow	X	X	X	X	Enable Disable	SO can configure the policy to enable a partition to be reset if it is locked as a result of exceeding the maximum number of failed login attempts.

[1] One and only one means of authentication ("user password" or "trusted path") must be enabled by the policy. Therefore, either one or both 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.

Description	Capability	S	SB	KEC	KES	Policy	Comments
	Disallow					Disable	A partition cannot be reset and must be re-created as a result of exceeding the maximum number of failed login attempts.
Network Replication	Allow					Enable	SO can configure the policy to enable the replication of the module's key material over the network to a second module.
						Disable	
	Disallow	X	X	X	X	Disable	The module cannot be replicated over the network.
Force user PIN change	Allow	X	X	X	X	Enable	This capability is set prior to shipment to the customer. If enabled, it forces the user to change PIN upon first login.
						Disable	
	Disallow					Disable	The user is never forced to change PIN on first login.
Remote authentication	Allow	X	X	X	X	Enable	This capability is set prior to shipment to the customer. It allows the use of remote authentication.
						Disable	
	Disallow					Disable	Remote authentication cannot be enabled for the module.

Table 3-2 Partition Capabilities and Policies

Description	Prerequisite	Capability	S	SB	KEC	KES	Policy	Comments
Level 3 operation without a challenge	Trusted path authentication enabled	Allow	X	X	X	X	Enable	SO can configure the policy to enable Level 3 login using the PED trusted path only, with no challenge-response validation required. Must be disabled if either activation or auto-activation is enabled
							Disable	
		Disallow					Disable	Challenge-response validation required plus PED trusted path login to access the partition.
User key management capability[2]	Trusted path authentication enabled, Level 3 operation without a challenge disabled	Allow	X	X	X	X	Enable	SO can configure the policy to enable the normal PKCS #11 user role to perform key management functions. If enabled, the Crypto Officer key management functions are available. If disabled, only the Crypto User role functions are accessible.
							Disable	
		Disallow					Disable	Only the Crypto User role functions are accessible.
Count failed challenge-response validations	Trusted path authentication enabled	Allow	X	X	X	X	Enable	SO can configure the policy to count failures of the challenge-response validation against the maximum login failures or not. Must be enabled if either activation or auto-activation is enabled
							Disable	
		Disallow					Disable	Failures of the challenge-response validation are not counted against the maximum login failures.

[2] This capability/policy is intended to offer customers a greater level of control over key management functions. By disabling the policy, the Security Officer places the partition into a state in which the key material is locked down and can only be used by connected applications, i.e., only Crypto User access is possible.

Description	Prerequisite	Capability	S	SB	KEC	KES	Policy	Comments
Activation	Trusted path authentication enabled	Allow					Enable Disable	SO can configure the policy to enable the authentication data provided via the PED trusted path to be cached in the module, allowing all subsequent access to the partition, after the first login, to be done on the basis of challenge-response validation alone.
		Disallow	X	X	X	X	Disable	PED trusted path authentication is required for every access to the partition.
Auto-activation	Trusted path authentication enabled	Allow					Enable Disable	SO can configure the policy to enable the activation data to be stored on the appliance server in encrypted form, allowing the partition to resume its authentication state after a re-start. This is intended primarily to allow partitions to automatically re-start operation when the appliance returns from a power outage.
		Disallow					Disable	Activation data cannot be externally cached.
High Availability	Network replication enabled	Allow	X	X	X	X	Enable Disable	SO can configure the policy to enable the use of the High Availability feature.
		Disallow					Disable	High Availability cannot be enabled.
Multipurpose keys	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the policy to enable the use of keys for more than one purpose, e.g., an RSA private key could be used for digital signature and for decryption. RSA key pairs generated using the X9.31 mechanism can only be used for signatures.
		Disallow					Disable	Keys can only be used for a single purpose.
Change attributes	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the policy to enable changing key attributes.
		Disallow					Disable	Key attributes cannot be changed.
Operate without RSA blinding	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the use of blinding mode for RSA operations. Blinding mode is used to defeat timing analysis attacks on RSA digital signature operations, but it also imposes a significant performance penalty on the signature operations.
		Disallow					Disable	Blinding mode is not used for RSA operations.

Description	Prerequisite	Capability	S	SB	KEC	KES	Policy	Comments
Signing with non-local keys	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the ability to sign with externally-generated private keys that have been imported into the partition.
		Disallow					Disable	Externally-generated private keys cannot be used for signature operations.
Raw RSA operations	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the ability to use raw (no padding) format for RSA operations.
		Disallow					Disable	Raw RSA cannot be used.
Private key wrapping	N/A	Allow			X	X	Enable Disable	SO can configure the ability to wrap private keys for export.
		Disallow	X	X			Disable	Private keys cannot be wrapped and exported from the partition.
Private key unwrapping	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the ability to unwrap private keys and import them into the partition.
		Disallow					Disable	Private keys cannot be unwrapped and imported into the partition.
Secret key wrapping	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the ability to wrap secret keys and export them from the partition.
		Disallow					Disable	Secret keys cannot be wrapped and exported from the partition.
Secret key unwrapping	N/A	Allow	X	X	X	X	Enable Disable	SO can configure the ability to unwrap secret keys and import them into the partition.
		Disallow					Disable	Secret keys cannot be unwrapped and imported into the partition.
Private key cloning	Cloning enabled, Trusted path authentication enabled	Allow					Enable Disable	SO can configure the ability to clone private keys from one partition to another.
		Disallow	X	X	X	X	Disable	Private keys cannot be cloned.
Secret key cloning	Cloning enabled, Trusted path authentication enabled	Allow			X		Enable Disable	SO can configure the ability to clone secret keys from one partition to another.
		Disallow	X	X		X	Disable	Secret keys cannot be cloned.
Private key masking	Masking enabled	Allow		X			Enable Disable	SO can configure the ability to mask private keys for storage outside the partition.
		Disallow	X		X	X	Disable	Private keys cannot be masked for storage outside the partition.
Secret key masking	Masking enabled	Allow		X		X	Enable Disable	SO can configure the ability to mask secret keys for storage outside the partition.
		Disallow	X		X		Disable	Secret keys cannot be masked for storage outside the partition.

Description	Prerequisite	Capability	S	SB	KEC	KES	Policy	Comments
RA type wrapping	Private key wrapping enabled	Allow			X	X	Enable Disable	This setting allows wrapping of individual private key CRT components rather than as one PKCS #8 formatted object.
		Disallow	X	X			Disable	
Minimum/maximum password length	User password authentication enabled	7-16 characters					Configurable	The SO can configure the minimum password length for Level 2 modules, but minimum length must always be >= 7.
Number of failed Partition User logins allowed	N/A	10					Configurable	The SO can configure; default maximum value is 10.

3.2. FIPS-Approved Mode

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

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

Additionally, for operation at **FIPS Level 2**, "User password authentication" must be enabled (implies that trusted path authentication is disallowed or disabled).

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

If the SO selects policy options (i.e., enables "Non-FIPS Algorithms Available") that would place the 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 determine FIPS mode of operation by matching the displayed capability and policy settings to those described in Sections 3.1 and 3.2.

3.3. Description of Operator, Subject and Object

3.3.1. Operator

An operator is defined as an entity that acts to perform an operation on the 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 the cryptographic module as part of the company's service. The operator might be that individual or group, particularly if they are interacting with the module locally. The operator might also be the composite of the individual or group, who might still be present locally to the module (particularly for activation purposes, see CR-2371, Level 3 Security Policy for Luna® CA[4] Cryptographic Module), plus the CA application running on a network-attached host computer.

3.3.2. Roles

In a Level 2 configuration (Password Authentication), the Luna PCM supports two authenticated roles: Crypto Officer and Security Officer. It also supports one unauthenticated operator role, the Public User, primarily to permit access to status information and diagnostics before authentication.

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

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 Crypto Officer or Security Officer role before identification and authentication;
- No identity can assume the Crypto Officer plus the Security Officer role.

3.3.3. Account Data

The module maintains the following User (per Partition[3]) and SO account data:

- Partition ID or SO ID number.
- Partition User encrypted or SO encrypted authentication data (checkword).
- Partition User locked out flag.

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

1. Only the Security Officer role can create (initialize) and delete the following security attributes:
   - Partition ID.
   - Checkword.
2. If Partition reset is allowed and enabled, the SO role only can modify the following security attribute:
   - Locked out flag for Partition User.
3. Only the Partition User can modify the following security attribute:
   - Checkword for Partition User.
4. Only the Security Officer role can change the default value, query, modify and delete the following security attribute:
   - Checkword for Security Officer.

[3] A Partition effectively represents an identity within the module.

3.3.4. Subject

For 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 the module and the processing of commands within the 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 the module associated with the same Access ID/Partition ID combination. It is also possible for the module to have sessions opened for more than one Partition ID or have multiple Access IDs with sessions opened on the module. Applications running on remote host systems that require data and cryptographic services from the 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 the module. A local application (e.g., command line administration interface) will open a session directly with the appropriate partition within the module without invoking the communications service.

3.3.5. 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 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.

3.3.6. 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.

3.3.7. Object Operations

Object operations may only be performed by a Partition User. New objects can be made in several ways. The following list identifies operations that produce new objects:

- Create,
- Copy,
- Generate,
- Unwrapping,
- 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. Operators are not given direct access to key values for any purpose.

3.4. Identification and Authentication

3.4.1. Authentication Data Generation and Entry

The module requires that Partition Users and the SO be authenticated by proving knowledge of a secret shared by the operator and the module.

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

3.4.2. Limits on Login Failures

The module also implements a maximum login attempts policy. The policy differs for an SO authentication data search and a Partition User authentication data search.

In the case of an SO authentication data search:

- If three (3) consecutive SO logon attempts fail, the module is zeroized.

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

1. If "Partition reset" is Allowed and Enabled, then if "n" ("n" is set by the SO at the time the HSM is initialized) consecutive operator logon attempts fail, the module flags the event in the Partition User's account data, locks the Partition User and clears the volatile memory space. The SO must unlock the partition in order for the Partition User to resume operation.
2. If "Partition reset" is not Allowed or not Enabled, then if "n" consecutive Partition User logon attempts via the physical trusted path fail, the module will erase the partition. The SO must delete and re-create the partition. Any objects stored in the partition, including private and secret keys, are permanently erased.

3.5. Access Control

The Access Control Policy is the main security function policy enforced by the module. It governs the rights of a subject to perform privileged functions and to access objects stored in the module. It covers the object operations detailed in section 3.3.7.

A subject's access to objects stored in the 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
  - 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 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 the module using the Wrap operation if allowed and enabled in the partition's policy set. Table 3-3 summarizes the object attributes used in Access Control Policy enforcement.

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

Attribute	Values	Impact
PRIVATE	TRUE – Object is private to (owned by) the operator identified as the Access Owner when the object is created.	Object is only accessible to subjects (sessions) bound to the operator identity that owns the object.
	FALSE – Object is not private to one operator identity.	Object is accessible to all subjects associated with the partition in which the object is stored.
SENSITIVE	TRUE – Attribute values representing plaintext key material are not permitted to exist (value encrypted).	Key material is stored in encrypted form.
	FALSE – Attribute values representing plaintext data are permitted to exist.	Plaintext data is stored with the object and is accessible to all subjects otherwise permitted access to the object.

[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.

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

Attribute	Values	Impact
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 Luna PCM using the Wrap operation.	The ability to extract a key permits sharing with other cryptomodules and archiving of key material.
	FALSE – Key material stored with the object may not be extracted from the Luna PCM.	Keys must never leave the module's control.

The module does not allow any granularity of access other than owner or non-owner (i.e., a Private object is only accessible by one Partition User. It 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 HSM 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:
  1. The object is a "Public" object, i.e., the PRIVATE attribute is FALSE, or
  2. The subject is bound to the Partition User that owns the object.
- Allowed operations are those permitted by the object attribute definitions within the constraints imposed by the HSM and Partition Capability and Policy settings.

3.5.1. 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.

3.5.2. Privileged Functions

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

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

3.6. 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:

(1) Pseudo random number generation in accordance with ANSI X9.31, Appendix A2.4.

(2) Cryptographic key generation in accordance with the following indicated standards:

a. RSA-1024-4096 bits key pairs in accordance with FIPS PUB 186-2.

b. TDES 112, 168 bits (FIPS PUB 46-3, ANSI X9.52).

c. AES 128, 192, 256 bits (FIPS PUB 197).

d. DSA 1024 bits key pairs in accordance with FIPS PUB 186-2.

e. ECDSA in accordance with ANSI X9.62.

(3) Secure key storage and key access.

(4) Destruction of cryptographic keys is performed in one of three ways as described below:

a. An object on the Luna PCM that is destroyed using the PKCS #11 function C_DestroyObject is marked invalid and remains encrypted with the Partition User's key or the Luna PCM's general secret key until such time as its memory locations (flash or RAM) are re-allocated for additional data on the Luna PCM, at which time they are purged and zeroized before re-allocation.

b. Objects on the Luna PCM 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 the Luna PCM are zeroized.

c. Objects on the Luna PCM that are destroyed through C_InitToken (the SO-accessible command to initialize the Luna PCM 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 secret key. 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 the module using the Unwrap, Unmask (if cloning is enabled at the HSM 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 the module and their attributes are set by the module to values required by the Access Control Policy.

3.7. Cryptographic Operations

Because of its generic nature, the module firmware supports 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:

(1) Symmetric encryption/decryption (and key wrap/unwrap): TDES 112, 168 bits (FIPS PUB 46-3, ANSI X9.52).

(2) Symmetric encryption/decryption (and key wrap/unwrap): AES 128, 192, 256 bits (FIPS PUB 197).

(3) Asymmetric key wrap/unwrap: RSA 1024 – 4096 (PKCS #1 V1.5)

(4) Signature generation/verification: RSA 1024-4096 bits (PKCS #1 V1.5) with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 180-2), RSA 1024-4096 bits (PSS) with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 180-2), RSA 1024-4096 bits (X9.31) with SHA-1, DSA 1024 bits (FIPS PUB 186-2) with SHA-1, ECDSA (ANSI X9.62) with SHA-1.

(5) Hash generation SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 180-2).

(6) Keyed hash generation HMAC using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 198).

(7) Message authentication TDES MAC (FIPS PUB 113)

(8) Pseudorandom number generation (ANSI X9.31 A2.4)

3.8. 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.

3.9. Firmware Security

The Firmware Security Policy assumes that any firmware images loaded in conformance with the policy have been verified by SafeNet 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[5] 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 SafeNet module dedicated to that function. Firmware shall be digitally signed using the SafeNet Manufacturing signature key and encrypted using a secret key that may be derived by the receiving module for decryption. The unencrypted firmware must not be visible outside the module before, during and after the loading operation. The target module shall verify the signature on the firmware image before allowing it to be loaded. If the signature does not verify, the module will return an error and not load the image. In the case of an attempted firmware update, it will continue to operate with the existing installed image.

The firmware shall provide mechanisms to ensure its own integrity and to ensure the integrity of any permanent security-critical data stored within the module.

3.10. Physical Security

The Luna PCM cryptographic module is a multi-chip standalone module as defined by FIPS PUB 140-2 section 4.5. It is enclosed in a strong enclosure that provides tamper-evidence. Any tampering that might compromise the module's security is detectable by visual inspection of the physical integrity of the module.

The module's physical design also resists visual inspection of the device design, physical probing of the device and attempts to access sensitive data on individual components of the device.

[5] External software means any form of executable code that has been generated by anyone other than SafeNet and has not been properly formatted and signed as a legitimate SafeNet firmware image.

3.11. Fault Tolerance

If power is lost to the 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.

The module shall maintain its secure state[6] 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.

3.12. Mitigation of Other Attacks

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

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

APPENDIX A. CRYPTOGRAPHIC ALGORITHMS SUPPORT

FIPS-approved algorithms are shown in bold lettering.

Encrypt/Decrypt:

- **TDES-ECB**
- **TDES-CBC**
- **AES-ECB**
- **AES-CBC**
- DES-ECB
- DES-CBC
- RC2-ECB
- RC2-CBC
- RC4
- RC5-ECB
- RC5-CBC
- CAST-ECB
- CAST-CBC
- CAST3-ECB
- CAST3-CBC
- CAST5-ECB
- CAST5-CBC
- RSA X-509
- SEED

Digest:

- **SHA-1**
- **SHA-256**
- **SHA-224**
- **SHA-384**
- **SHA-512**
- MD2
- MD5
- HAS-160

Sign/Verify:

- **RSA-1024-4096 X9.31**
- **RSA-1024-4096 PKCS #1 V1.5 with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**
- **RSA-1024-4096 PSS with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**
- **DSA-1024**
- **ECDSA**
- **TDES-MAC**
- **HMAC-SHA1**
- **HMAC-SHA-224**
- **HMAC-SHA-256**
- **HMAC-SHA-384**
- **HMAC-SHA-512**
- AES-MAC
- DES-MAC
- RC2-MAC
- RC5-MAC
- CAST-MAC
- CAST3-MAC
- CAST5-MAC
- SSL3-MD5-MAC
- SSL3-SHA1-MAC
- HMAC-MD5
- KCDSA

Generate Key:

- **2Key TDES**
- **3Key TDES**
- **AES 128, 192, 256 bits**
- DES
- RC2
- RC4
- RC5
- CAST
- CAST3
- CAST5
- SEED
- PBE-MD2-DES
- PBE-MD5-DES
- PBE-MD5-CAST
- PBE-MD5-CAST3
- PBE-SHA-1-CAST5
- GENERIC-SECRET
- SSL PRE-MASTER

Generate Key Pair:

- **RSA-1024 – 4096 X9.31 and PKCS #1**
- **DSA-1024**
- **ECDSA (NIST curves)**
- DH-1024 – provides 80-bits of encryption strength
- KCDSA

Wrap Symmetric Key Using Symmetric Algorithm:

- **TDES-ECB**
- **AES-ECB**
- RC2-ECB
- CAST-ECB
- CAST3-ECB
- CAST5-ECB

Wrap Symmetric Key Using Asymmetric Algorithm:

- **RSA-1024 – provides 80-bits of encryption strength**
- **RSA-2048 – provides 112-bits of encryption strength**
- **RSA-4096 – provides 150-bits of encryption strength**

Wrap Asymmetric Key Using Symmetric Algorithm:

- **TDES-CBC**
- **AES-CBC**

Unwrap Symmetric Key With Symmetric Algorithm:

- **TDES-ECB**
- **AES ECB**
- RC2-ECB
- CAST-ECB
- CAST3-ECB
- CAST5-ECB

Unwrap Symmetric Key With Asymmetric Algorithm:

- **RSA-1024**
- **RSA-2048**
- **RSA-4096**

Unwrap Asymmetric Key With Symmetric Algorithm:

- **TDES-CBC**
- **AES-CBC**
- CAST-CBC
- CAST3-CBC
- CAST5-CBC

APPENDIX B. SECURITY POLICY CHECKLIST TABLES

Table B-1 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Security Officer	Role-based	Level 2 – Password
Crypto Officer	Role-based	Level 2 – Password
Public User	Not required	N/A

Table B-2 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password (Level 2)	Configurable by SO from 7 to 16 characters

Table B-3 Services Authorized for Roles

Role	Authorized Services
Security Officer	Show Status, Self-test, Initialize Module, Configure Module Policy, Create Partition, Configure Partition Policy, Key and Key Pair Generation, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Symmetric & Asymmetric Key Wrap/Unwrap, Symmetric & Asymmetric Key Mask/Unmask, Store Data Object, Read Data Object, HSM Backup and Restore
Crypto Officer	Show Status, Self-test, Key and Key Pair Generation, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Symmetric & Asymmetric Key Wrap/Unwrap, Symmetric & Asymmetric Key Mask/Unmask, Store Data Object, Read Data Object, Partition Backup and Restore
Public User	Show Status, Self-test

Table B-4 Access Rights within Services

Service	Cryptographic Keys and CSPs	Role	Type(s) of Access
Show Status	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[7]
Create Partition	Authentication data via trusted path	SO	Write – User authentication data
Configure Partition Policy	Authentication data via trusted path	SO	Use
HSM Backup/Restore	Module Masking Secret	SO	Transfer[11]
Key and Key Pair Generation	Symmetric keys, asymmetric key pairs	SO, Crypto Officer	Write
Symmetric Key Wrap/ Unwrap	Symmetric with RSA Symmetric with Symmetric ECB mode	SO, Crypto Officer	Use, Write
Asymmetric Key Wrap/ Unwrap	Asymmetric with Symmetric CBC mode	SO, Crypto Officer	Use, Write
Symmetric Key Mask/ Unmask	Symmetric with AES 256	SO, Crypto Officer	Use, Write
Asymmetric Key Mask/ Unmask	Symmetric with AES 256	SO, Crypto Officer	Use, Write
Partition Backup/Restore	Symmetric keys, asymmetric key pairs	Crypto Officer	Transfer[8]
Symmetric Encrypt/Decrypt	Symmetric keys	SO, Crypto Officer	Use
Asymmetric Signature	RSA, DSA private keys	SO, Crypto Officer	Use
Asymmetric Verification	RSA, DSA public keys	SO, Crypto Officer	Use
Store Data Object	Non-cryptographic data	SO, Crypto Officer	Write
Read Data Object	Non-cryptographic data	SO, Crypto Officer	Read

Table B-5 Keys and Critical Security Parameters Used in the Module

Key/CSP Name	Description
SIM authorization values	These M of N secret values are used to authorize the insertion of a masked key blob previously extracted using the SIM II feature.
User password	Used in Password Authentication (Level 2) configuration only. The user provided password used for authentication in a Level 2 configuration. Minimum of 7 characters and maximum of 16.
RNG Seed Value (V)	The 64 bit intermediate value of the X9.31 Annex A2.4 TDES-based PRNG algorithm. It is used as one of the initial seed values for the algorithm.
RNG Key Value (*K)	The double-length TDES key used for the X9.31 Annex A2.4 TDES-based PRNG algorithm. It is used as one of the initial seed values for the algorithm.
Cloning Domain Vector	24-byte value that is used to control a module's ability to participate in the cloning protocol.
User Storage Key (USK)	24-byte TDES key that is randomly generated for each user on a Luna PCM. This key is used to encrypt all sensitive attributes of all private objects owned by the user.

[7] Use means access to key material for use in performing a cryptographic operation. The key material is never visible.
[8] Transfer means moving a key using the cloning protocol from one crypto module to another.

Table B-5 Keys and Critical Security Parameters Used in the Module

Key/CSP Name	Description
Security Officer Master Key (SMK)	The storage key for the SO; a 24-byte TDES key that is randomly generated for the SO on the module. This key is used to encrypt all sensitive attributes of all private objects owned by the SO. The USK/SMK is stored encrypted using an AES key, which is derived from the User/SO password.
Global Storage Key (GSK)	24-byte TDES key that is the same for all users on a specific Luna PCM. It is stored encrypted with USK and SMK. It is used to encrypt permanent parameters within the non-volatile memory area reserved for use by the module.
Secondary Global Storage Key (SGSK)	24-byte TDES key that is the same for all users on a specific Luna PCM. It is stored encrypted using USK and SMK. It is used to encrypt non-permanent parameters (parameters re-generated for every module initialization) within the non-volatile memory area reserved for use by the module.
Token or Module Signing Key (TSK)	A 1024-bit RSA private key used in the cloning protocol. Stored in the Param area.
Token or Module Wrapping Key (TWK)	1024-bit RSA public key used in exchange of session encryption key as part of the handshake during the cloning protocol. Stored in the Param area.
U Key	24-byte TDES 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. Stored in the Param area.
Token or Module Variable Key (TVK)	24-byte TDES key stored in a dedicated non-volatile RAM. It is used to encrypt authentication data stored for auto-activation purposes.
Masking Key	AES 256-bit key stored in the Param area. It is generated on the HSM at initialization time. It is used during masking operations
Manufacturers Verification Key (MVK)	4096-bit Public key counterpart to the Manufacturer Signature Key held at SafeNet Canada. Used to verify the digital signature on a firmware update image.
Hardware Origin Key (HOK)	4096-bit RSA private key used in applications requiring assurance that a key or a specific action originated within the hardware crypto module.
Device Authentication Key (DAK)	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.

- THIS PAGE LEFT BLANK INTENTIONALLY -

APPENDIX C. LIST OF TERMS, ABBREVIATIONS AND ACRONYMS

Term	Definition
ANSI	American National Standards Institute
CA	Certification Authority
Chrysalis-ITS	Former name of SafeNet Canada, Inc.
CRT	Chinese Remainder Theorem
DAK	Device Authentication Key
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standard
GSK	Global Storage Key
HA	High Availability
HOK	Hardware Origin Key
HSM	Hardware Security Module
KEC	Key Export - Cloning
KES	Key Export - SIM
MAC	Message Authentication Code
MVK	Manufacturers Verification Key
PCMCIA	Personal Computer Memory Card Industry Association
PKCS	Public-Key Cryptography Standards
PED	PIN Entry Device
PRNG	Pseudo-Random Number Generator
RA	Registration Authority
RNG	Random Number Generator
S	Signing
SB	Signing with Backup
SGSK	Secondary Global Storage Key
SIM	Secure Information Management
SMK	Security Officer Master Key
SO	Security Officer
TSK	Token or Module Signing Key
TVK	Token or Module Variable Key
TWK	Token or Module Wrapping Key
USK	User's Storage Key

- THIS PAGE LEFT BLANK INTENTIONALLY -