LEVEL 3 SECURITY POLICY FOR

Luna® K4 Cryptographic Module

and

NITROX XL CN1120-NFB Acceleration Board, NITROX XL CN1010- NFB Acceleration Board, NITROX XL CN1005- NFB Acceleration Board

DOCUMENT NUMBER:	CR-2044
AUTHOR:	Terry Fletcher
DEPARTMENT:	Engineering
LOCATION OF ISSUE:	Ottawa
DATE ORIGINATED:	December 9, 2004
REVISION LEVEL:	2
REVISION DATE:	July 7, 2005
SUPERSESSION DATA:	CR-2044, 1
SECURITY LEVEL:	

SafeNet Canada, Inc. reserves the right to make changes in the product or its specifications mentioned in this publication without notice. Accordingly, the reader is cautioned to verify that information in this publication is current before placing orders. The information furnished by SafeNet Canada, Inc. in this document is believed to be accurate and reliable. However, no responsibility is assumed by SafeNet Canada, Inc. for its use, or for any infringements of patents or other rights of third parties resulting from its use. No part of this publication may be copied or reproduced in any form or by any means, or transferred to any third party without prior written consent of SafeNet Canada, Inc.

TABLE OF CONTENTS

Section **Title** **Page**

LIST OF TABLES

Table **Title** **Page**

LIST OF FIGURES

Figure **Title** **Page**

LIST OF APPENDICES

Appendix **Title** **Page**

1. INTRODUCTION

1.1. Purpose

This document describes the security policies enforced by SafeNet Canada Inc.’s Luna® K4 Cryptographic Module, also known as the K4.

This document also applies to Cavium Network’s NITROX XL CN1120-NFB Acceleration Board, NITROX XL CN1010-NFB Acceleration Board, and NITROX XL CN1005-NFB Acceleration Board. The SafeNet and Cavium K4 modules are identical, except that the Cavium K4 has a limited subset of policy items that are configurable by the Security Officer when the module is initialized.

This document applies to Hardware Versions VBD-02-0200 and VBD-02-0201 and Firmware Version 4.3.5.

1.2. Scope

The security policies described in this document apply to the SafeNet and Cavium configurations of the K4 Cryptographic Module only and do not include any security policy that may be enforced by the host appliance.

2. SECURITY POLICY MODEL INTRODUCTION

2.1. Functional Overview

The K4 cryptographic module is a multi-chip embedded hardware cryptographic module in the form of a PCI 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 and zeroization of plaintext key material and security parameters in the event the enclosure is opened. The cryptographic boundary of the module is defined to encompass all components inside the secure enclosure on the PCI card. Figure 2-1 depicts the K4 cryptographic module.

The module may be explicitly configured to operate in either FIPS Level 2 or FIPS Level 3 mode, or in a non-FIPS mode of operation. Configuration in either FIPS mode enforces the use of FIPS-approved algorithms only. Configuration in FIPS Level 3 mode also enforces the use of trusted path authentication. Note that selection of FIPS mode occurs at initialization of the HSM, and cannot be changed during normal operation without zeroizing the module’s non-volatile memory.

The cryptographic module is accessed directly (i.e., electrically) via either the Trusted Path PIN Entry Device (PED) serial interface or via the PCI 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.

The K4 module may be configured and sold as either a SafeNet or a Cavium product. The SafeNet and Cavium K4 modules are identical, except that the Cavium K4 has a limited subset of policy items that are configurable by the Security Officer when the module is initialized.

This Security Policy is specifically written for the K4 in a **FIPS Level 3** configuration.

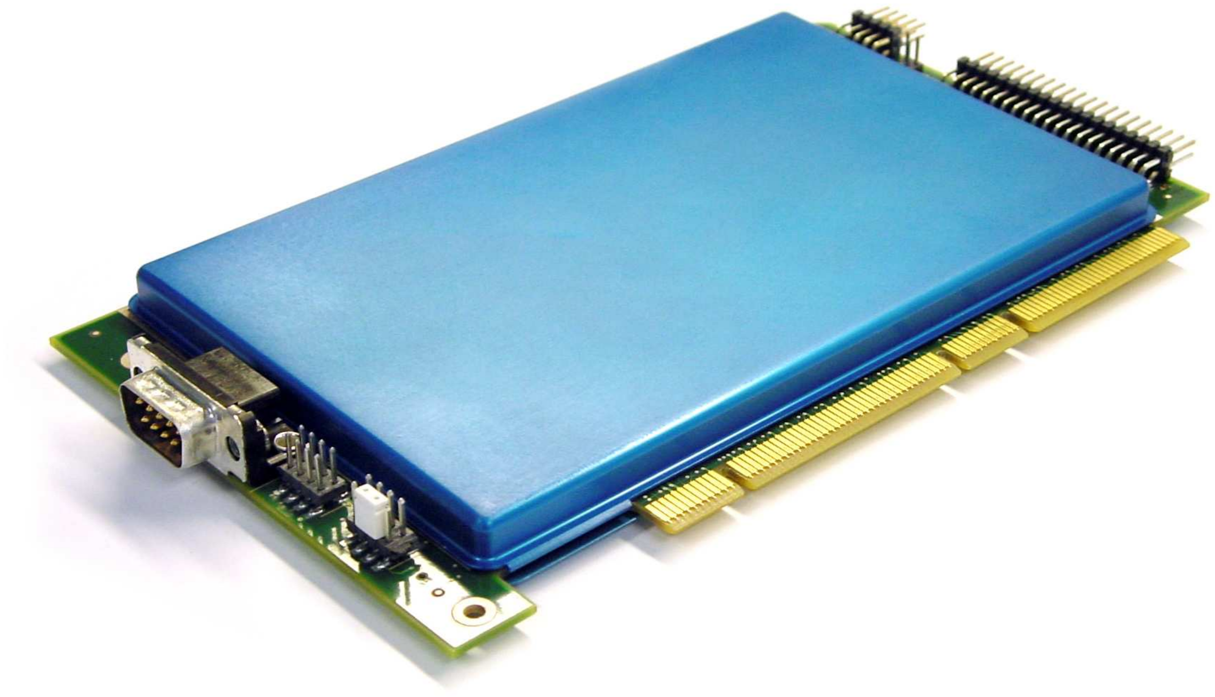

Figure 2-1. K4 Cryptographic Module

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 within 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.

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. Note that the current version of the K4 only supports a single partition. 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 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.

The operational policy configurable settings for the Cavium K4 module are described in Appendix C. The remainder of this section describes the full set of HSM and partition level capabilities available in the K4 firmware; only a subset of these is configurable for Cavium modules.

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. (Disallowed in Level 3 configuration.)
- Allow/disallow trusted path authentication.
- Allow/disallow M of N. (Disallowed in Cavium K4.)
- Allow/disallow cloning.
- Allow/disallow masking.
- Allow/disallow M of N auto-activation. (Disallowed in Cavium K4.)
- Allow/disallow domestic algorithms and key sizes available. (Default is Allow.)
- Allow/disallow modification of personality licenses. (Disallowed in Cavium K4.)
- Allow/disallow modification of capabilities[1].
- Allow/disallow ECC mechanisms. (Disallowed in Cavium K4.)
- Performance level (4 bits), see section 3.12.
- Number of failed SO logins allowed before the HSM is zeroized (set to 3).
- Allow/disallow Korean Digital Signature algorithms. (Disallowed in Cavium K4.)
- Allow/disallow Remote Authentication. (Disallowed in Cavium K4.)
- Allow/disallow SO reset of partition PIN.
- Allow disallow network replication. (Disallowed in Cavium K4.)
- Allow/disallow forcing PIN change. (Disallowed in Cavium K4.)
- Allow/disallow special cloning certificate. (Disallowed in Cavium K4.)

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 HA (High Availability). (Disallowed in Cavium K4.)
- Allow/disallow multipurpose keys.

[1] This module capability exists only to permit programming of capabilities at SafeNet in the event that appropriate licensing is not possible. It will always be set to “disallowed” when the module is delivered to the customer.

- 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. (Disallowed in Cavium K4.)
- Allow/disallow private key unwrapping.
- Allow/disallow secret key wrapping
- Allow/disallow secret key unwrapping.
- Allow/disallow Level 3 operation without a challenge.
- Allow/disallow user key management capability.
- Allow/disallow all functionality in excess of that implemented by backup tokens.
- Allow/disallow incrementing of failed login attempt counter on failed challenge response validation.
- Allow/disallow RSA signing without confirmation
- Allow/disallow RA type wrapping. (Disallowed in Cavium K4.)
- Level of storage space available for key storage (4 bits).
- Minimum/maximum password length (applies only to Level 2 modules and minimum must be >= 7).
- Number of failed Partition User logins allowed before partition is locked out/cleared.

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

- Allow/disallow private key cloning. (Disallowed in Cavium K4.)
- Allow/disallow secret key cloning. (Disallowed in Cavium K4.)

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.

Table 3-1 Module Capabilities and Policies

Description	Capability	Policy	Comments
Non-FIPS algorithms available	Allow	Enable	SO can configure the policy to enable or disable the availability of non-FIPS algorithms at the time the HSM is initialized.
		Disable	
	Disallow	Disable	The HSM 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	Disable	The HSM must operate using the trusted path and module-generated secrets for authentication.
Trusted path authentication	Allow	Enable	SO can configure the policy to enable or disable the use of the trusted path and module-generated secrets for authentication.
		Disable	
	Disallow	Disable	The HSM must operate using passwords without trusted path for authentication.[2]
M of N	Allow	N/A	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		The HSM must operate without M of N secret sharing for activation.
Cloning	Allow	Enable	SO can configure the policy to enable or disable the availability of the cloning function for the HSM as a whole.
		Disable	
	Disallow	Disable	The HSM must operate without cloning.
Masking	Allow	Enable	SO can configure the policy to enable or disable the availability of the masking function for the HSM as a whole.
		Disable	
	Disallow	Disable	The HSM must operate without masking.
M of N auto-activation	Allow	N/A	SO can configure the policy to enable or disable the use of the M of N auto-activation feature.
	Disallow		The HSM must operate without M of N auto-activation.
Domestic product algorithms and key sizes available	Allow	N/A	This capability is set prior to shipment to the customer. It controls the availability of domestic strength algorithms and key sizes. The default setting is Allow.
	Disallow		
Modification of personality licenses	Allow	N/A	This capability is set prior to shipment to the customer. It controls the ability to modify partition personality licenses in the field. The default setting is Disallow.
	Disallow		
Modification of capabilities	Allow	N/A	This capability is set prior to shipment to the customer. It controls the ability to modify the capability set in the field. This capability will only be set to Allow for SafeNet use; it will always be set to Disallow for a module shipped to a customer.
	Disallow		
ECC mechanisms available	Allow	N/A	This capability is set prior to shipment to the customer. It controls the availability of ECC mechanisms. The default setting is Disallow.
	Disallow		
Partition reset	Allow	Enable	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.
		Disable	
	Disallow	Disable	A partition cannot be reset and must be re-created as a result of exceeding the maximum number of failed login attempts.

[2] 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.

Table 3-1 Module Capabilities and Policies

Description	Capability	Policy	Comments
Network Replication	Allow	N/A	SO can configure the policy to enable the replication of the module's key material over the network to a second module.
	Disallow		The module cannot be replicated over the network.
Non-backup token functions	Allow	Enable	Applies to G3 token-based modules. SO can enable full functionality for the token or simple backup functionality only.
		Disable	
	Disallow	Disable	Backup functionality only is allowed.
Korean Digital Signature Algorithm	Allow	N/A	This capability is set prior to shipment to the customer. It controls the availability of Korean Digital Signature Algorithms. The default setting is Disallow.
	Disallow		
Force user PIN change	Allow	N/A	This capability is set prior to shipment to the customer. It forces the user to change PIN upon first login. The default setting is Disallow.
	Disallow		
Special cloning certificate	Allow	N/A	This capability is set prior to shipment to the customer. It allows the use of special (non-HSM) certificates for cloning. The default setting is Disallow.
	Disallow		
Remote authentication	Allow	N/A	This capability is set prior to shipment to the customer. It allows the use of remote authentication. The default setting is Disallow.
	Disallow		

Table 3-2 Partition Capabilities and Policies

Description	Prerequisite	Capability	Policy	Comments
Level 3 operation without a challenge	Trusted path authentication enabled	Allow	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[3]	Trusted path authentication enabled, Level 3 operation without a challenge disabled	Allow	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	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.

[3] 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.

Table 3-2 Partition Capabilities and Policies

Description	Prerequisite	Capability	Policy	Comments
Activation	Trusted path authentication enabled	Allow	Enable	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.
			Disable	
		Disallow	Disable	PED trusted path authentication is required for every access to the partition.
Auto-activation	Trusted path authentication enabled	Allow	Enable	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.
			Disable	
		Disallow	Disable	Activation data cannot be externally cached.
High Availability	N/A	Allow	N/A	SO can configure the policy to enable the use of the High Availability login feature. This allows a partition in one appliance to act as a trusted remote authentication device for one or more partitions in remotely connected appliances. High Availability login is disallowed in Cavium K4.
		Disallow		
Multipurpose keys	N/A	Allow	Enable	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.
			Disable	
		Disallow	Disable	Keys can only be used for a single purpose.
Change attributes	N/A	Allow	Enable	SO can configure the policy to enable changing key attributes.
			Disable	
		Disallow	Disable	Key attributes cannot be changed.
Operate without RSA blinding	N/A	Allow	Enable	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.
			Disable	
		Disallow	Disable	Blinding mode is not used for RSA operations.
Signing with non-local keys	N/A	Allow	Enable	SO can configure the ability to sign with externally-generated private keys that have been imported into the partition.
			Disable	
		Disallow	Disable	Externally-generated private keys cannot be used for signature operations.
Raw RSA operations	N/A	Allow	Enable	SO can configure the ability to use raw (no padding) format for RSA operations.
			Disable	
		Disallow	Disable	Raw RSA cannot be used.
Private key wrapping	N/A	Allow	N/A	Private keys cannot be wrapped and exported from the partition in a Cavium K4.
		Disallow		

Table 3-2 Partition Capabilities and Policies

Description	Prerequisite	Capability	Policy	Comments
Private key unwrapping	N/A	Allow	Enable	SO can configure the ability to unwrap private keys and import them into the partition.
			Disable	
		Disallow	Disable	Private keys cannot be unwrapped and imported into the partition.
Secret key wrapping	N/A	Allow	Enable	SO can configure the ability to wrap secret keys and export them from the partition.
			Disable	
		Disallow	Disable	Secret keys cannot be wrapped and exported from the partition.
Secret key unwrapping	N/A	Allow	Enable	SO can configure the ability to unwrap secret keys and import them into the partition.
			Disable	
		Disallow	Disable	Secret keys cannot be unwrapped and imported into the partition.
Private key cloning	Cloning enabled, Trusted path authentication enabled	Allow	N/A	Private keys cannot be cloned from one partition to another in the same domain in the Cavium K4.
		Disallow		
Secret key cloning	Cloning enabled, Trusted path authentication enabled	Allow	N/A	Secret keys cannot be cloned from one partition to another in the same domain in the Cavium K4.
		Disallow		
Private key masking	Masking enabled	Allow	Enable	SO can configure the ability to mask private keys for storage outside the partition.
			Disable	
		Disallow	Disable	Private keys cannot be masked for storage outside the partition.
Private key unmasking	Masking enabled	Allow	Enable	SO can configure the ability to unmask private keys and retrieve them into the partition.
			Disable	
		Disallow	Disable	Private keys cannot be unmasked and retrieved into the partition.
Secret key masking	Masking enabled	Allow	Enable	SO can configure the ability to mask secret keys for storage outside the partition.
			Disable	
		Disallow	Disable	Secret keys cannot be masked for storage outside the partition.
Secret key unmasking	Masking enabled	Allow	Enable	SO can configure the ability to unmask secret keys and retrieve them into the partition.
			Disable	
		Disallow	Disable	Secret keys cannot be unmasked and retrieved into the partition.
Storage space	N/A	N/A	N/A	N/A
Minimum/maximum password length	User password authentication enabled	7-16 characters	Configurable	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	SO can configure; default maximum value is 10.
RA type wrapping	Private key wrapping enabled	Allow	N/A	This setting allows wrapping of individual private key CRT components rather than as one PKCS #8 formatted object. Disallowed in Cavium K4
		Disallow		

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 3**:

- "Trusted path authentication" must be enabled (implies that password authentication is disallowed or disabled), and
- "Level 3 operation without a challenge" must be disabled if activation or auto-activation is enabled.
- "Count failed challenge – response validations" must be enabled if activation or auto-activation is enabled.

The policy settings for "Trusted path 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 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 authentication purposes), plus the CA application running on a network-attached host computer.

3.3.2. Roles

In Level 3 mode (Trusted Path Authentication), the K4 cryptographic module supports three authenticated operator roles: Crypto User and Crypto Officer for each partition (collectively called the Partition Users), plus the Security Officer at the module level. In Level 2 mode (Password Authentication), it supports two authenticated roles: Crypto Officer for each partition 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 role for each partition and the Crypto User is an optional read-only role that limits the operator to performing cryptographic operations only. In Level 2 mode, the Crypto Officer role is the only authenticated user role.

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

The SO 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” policy.

3.3.3. Account Data

The module maintains the following Partition User (which can include both the Crypto Officer and Crypto User role for the partition) and SO account data:

- Partition ID[4] or SO ID number.
- Partition User encrypted or SO encrypted authentication data (checkword).
- Partition User authentication challenge secret (one for each role, as applicable).
- Partition User locked out flag.

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.

[4] Only one partition is supported in the Cavium K4.

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 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. 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 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.

3.3.6. 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. 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 3.5. 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;
- 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. 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. The FIPS mode (either level 2 or level 3) is determined when the HSM is initialized: A module that is to support level 2 mode must be initialized using a password to define the SO authentication data; a module that is to support level 3 mode must be initialized using the PED to define the SO authentication data.

For a module operating in FIPS Level 3 mode, the module generates the authentication secret as a 48-byte random value and, optionally, an authentication challenge secret. The authentication secret(s) are provided to the operator via a physically separate trusted path, described in sub-section 3.4.2, 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. Both the Crypto Officer and Crypto User use the same secret. If a Partition is created with Crypto Officer and Crypto User roles, a separate challenge secret is generated for each role.

3.4.2. Trusted Path

In FIPS Level 3 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) that is physically separate from the host IT environment. The primary form of authentication data used during Activation is the 48-byte value that is randomly generated by the module and stored on the Black (User) PED Key (serial memory device) via the physical trusted path. The data on the PED Key must then be entered into the 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 the 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 and for user authentication when the settings of the Partition Policy disable the use of challenge/response authentication for login to a partition[5], the presentation of the PED key 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 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 the 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.

[5] Challenge/response authentication might, for example, be disabled in a case where both the cryptographic module and the attached application server are located within a physically secured environment and the user is required to always be physically present to start the application and authenticate to the cryptographic module via the PED.

3.4.3. 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.

3.4.4. M of N Activation

If M of N activation is required by the Module Policy, “M” pieces out of a total of “N” pieces of a split authentication secret must be entered via the trusted path in order to activate the module for operation. The M of N secret and the splits are generated by the module. In the Cavium K4 module, M of N is disabled.

3.4.5. Remote Authentication

The Remote Authentication feature allows one K4 module operating in a Level 3 configuration to accept, via its PED, the PED key data (User or SO) for a second K4 module and to securely transfer the PED key data to the second module, where it is acted upon. The secure transfer is performed using the cloning protocol and ensures that both modules have been authenticated using a digital signature-based technique and that each transfer is encrypted using a separately negotiated TDES session key. In the Cavium K4 module, this feature is disabled.

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 following object operations:

- Create
- Read (Query Attribute Value)
- Copy
- Modify
- Destroy
- Generate
- Derive
- Wrap
- Unwrap

- Clone
- Mask
- Use

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[6].** 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. Sensitive objects are encrypted using the partition's secret key to prevent their values from ever being exposed to external entities. Key objects are always created as Sensitive objects and 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.
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.

[6] 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
EXTRACTABLE	TRUE – Key material stored with the object may be extracted from the K4 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 K4.	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 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 following constraints:
  1. A Partition User in the Crypto User role has access to only the Use operations, and
  2. The restrictions 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 512-1024 bits key pairs in accordance with FIPS PUB 186-2.

(3) Secure key storage and key access following the PKCS #11 standard.

(4) 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:

a. An object on the K4 that is destroyed using the PKCS #11 function C_DestroyObject is marked invalid and remains encrypted with the Partition User's key or the K4's general secret key until such time as its memory locations (flash or RAM) are re-allocated for additional data on the K4, at which time they are purged and zeroized before re-allocation.

b. Objects on the K4 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 K4 are zeroized.

c. Objects on the K4 that are destroyed through C_InitToken (the SO-accessible command to initialize the K4 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 (key wrap/unwrap) TDES 168 bits in accordance with PKCS #11.

(2) Symmetric encryption/decryption: DES 56 bits[7], TDES 112, 168 bits (FIPS PUB 46-3, ANSI X9.52).

(3) Symmetric encryption/decryption: AES 128, 192, 256 bits (FIPS PUB 197).

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

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

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

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

[7] DES must be used for legacy purposes only

(8) Random number generation (ANSI X9.31)

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.

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[8] 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 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 K4 cryptographic module is a multi-chip embedded module as defined by FIPS PUB 140-2 section 4.5. It is enclosed in a strong enclosure that provides tamper-evidence, and detection and response features. Any tampering that might compromise the module's security is detectable by visual inspection of the physical integrity of the module. Attempts to remove the enclosure are detected and the module responds by entering an inoperative state and erasing all plaintext sensitive data from volatile and non-volatile memory.

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.

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[9] 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. Performance Levels

The Cavium K4 may be manufactured in one of three different performance configurations: low, medium and high performance. The performance capability setting allows for a value of between 0 and 15. The settings used in the Cavium K4 are 2 for low performance, 4 for medium performance and 8 for high performance. Any value greater than 8 will also result in the high performance capability setting.

[8] 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.

[9] A secure state is one in which either the K4 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 K4.

3.13. 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.

APPENDIX A. CRYPTOGRAPHIC ALGORITHMS SUPPORT

FIPS-approved algorithms are shown in bold lettering.

Encrypt/Decrypt:

- **DES-ECB**
- **DES-CBC**
- **3-DES-ECB**
- **3-DES-CBC**
- **AES ECB**
- **AES 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-384**
- **SHA-512**
- MD2
- MD5

Sign/Verify:

- **RSA-1024-4096**
- **DSA 512-1024**
- **ECDSA**
- **DES-MAC**
- **3-DES-MAC**
- AES MAC
- **HMAC-SHA1**
- RC2-MAC
- RC5-MAC
- CAST-MAC
- CAST3-MAC
- CAST5-MAC
- SSL3-MD5-MAC
- SSL3-SHA1-MAC
- HMAC-MD5
- KCDSA

Generate Key:

- **DES**
- **2Key TDES**
- **3Key TDES**
- **AES 128, 192, 256 bits**
- 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**
- **RSA-2048**
- **RSA-4096**
- **DSA-1024**
- DH-1024
- KCDSA

Wrap Symmetric Key Using Symmetric Algorithm:

- **DES-ECB**
- **3-DES-ECB**
- **AES ECB**
- RC2-ECB
- CAST-ECB
- CAST3-ECB
- CAST5-ECB

Wrap Symmetric Key Using Asymmetric Algorithm:

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

Wrap Asymmetric Key Using Symmetric Algorithm:

- **3-DES-CBC**
- **AES-CBC**

Unwrap Symmetric Key With Symmetric Algorithm:

- **DES-ECB**
- **3-DES-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:

- **DES-CBC**
- **3-DES-CBC**
- **AES-CBC**
- CAST-CBC
- CAST3-CBC
- CAST5-CB

APPENDIX B. SECURITY POLICY CHECKLIST TABLES

Table B-1 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Security Officer	Identity-based	Level 2 – Password Level 3 – Authentication token (PED Key – one per module) plus optional PED PIN
Crypto Officer	Identity-based plus Role-based[10]	Level 2 – Password Level 3- Authentication token (PED Key – one per user) plus optional PED PIN, plus optional Challenge Secret for the role[11]
Crypto User	Identity-based plus Role-based	Level 2- Password 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 B-2 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password (Level 2)	Configurable by SO from 7 to 16 characters
PED Key (Level 3) plus PIN	48 byte random authentication data store on PED Key plus PIN entered via PED key pad (minimum 4 bytes)
Challenge Secret (Level 3)	16 character random string

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, 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, Store Data Object, Read Data Object, Partition Backup and Restore
Crypto User	Show Status, Self-test, Symmetric Encrypt/Decrypt, Asymmetric Signature/Verification, Store Data Object, Read Data Object
Public User	Show Status, Self-test

[10] 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.

[11] If activation or auto-activation is enabled, challenge secret is required in FIPS mode

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[12]
Create Partition	Authentication data via trusted path	SO	Write – User authentication data
Configure Partition Policy	Authentication data via trusted path	SO	Use
Key and Key Pair Generation	Symmetric keys, asymmetric key pairs	Crypto Officer	Write
Symmetric Key Wrap/ Unwrap	Symmetric with RSA Symmetric with Symmetric ECB mode	Crypto Officer	Use, Write
Asymmetric Key Wrap/ Unwrap	Asymmetric with Symmetric CBC mode	Crypto Officer	Use, Write
Symmetric Key Mask/ Unmask	Symmetric with AES 256	Crypto Officer	Use, Write
Asymmetric Key Mask/ Unmask	Symmetric with AES 256	Crypto Officer	Use, Write
Backup Keys	Symmetric keys, asymmetric key pairs	Crypto Officer	Transfer[13]
Symmetric Encrypt/Decrypt	Symmetric keys	Crypto Officer, Crypto User	Use
Asymmetric Signature	RSA, DSA private keys	Crypto Officer, Crypto User	Use
Asymmetric Verification	RSA, DSA public keys	Crypto Officer, Crypto User	Use
Store Data Object	Non-cryptographic data	Crypto Officer, Crypto User	Write
Read Data Object	Non-cryptographic data	Crypto Officer, Crypto User	Read

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

Key Name	Description
Challenge Secret	Used in Trusted Path Authentication (Level 3) configuration only. 16 character random string generated by the HSM 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	Used in Trusted Path Authentication (Level 3) configuration only. A one-time random number generated by the HSM 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 HSM.
Challenge Response	A 20-byte value used for authentication in the challenge response scheme. It generated using the challenge secret and the one-time random challenge value.

[12] Use means access to key material for use in performing a cryptographic operation. The key material is never visible.

[13] 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 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.
PED Key Authentication Data	48-byte random value that is generated by the module when the SO or User is created. It is written out to serial memory device (PED Key) via the Trusted Path.
Optional PIN	An optional PIN value used for authentication along with the PED key. It must be a minimum of 4-bytes long
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 K4. This key is used to encrypt all sensitive attributes of all private objects owned by the user.
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 the first 32 bytes of the User/SO PED Key Authentication data.
Global Storage Key (GSK)	24-byte TDES key that is the same for all users on a specific K4. 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 K4. 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 K4 Signing Key (TSK)	A 1024-bit RSA private key used in the cloning protocol. Stored in the Param area.
Token or K4 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 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. The non-volatile RAM is actively zeroized in response to a tamper event.
Masking Key	AES 256-bit key stored in the Param area. It is generated on

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

Key Name	Description
	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)	2048-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.

APPENDIX C. CAVIUM K4 SECURITY POLICY SUMMARY TABLE

The Cavium K4 is manufactured to support a range of security related applications. In addition, there are some optional capabilities that may be applied to the K4 as a Secure Capability Update (SCU) in the field. Please contact Cavium Networks for a list of available optional SCUs.

Capabilities may be either enabled or disabled by the Security Officer (SO) as a matter of establishing the security policies for the HSM. Although policy is generally applied at the time the K4 is initialized, it is possible for the SO to change policy as it supports the operational process. It is important to note however, that some policy changes are destructive in nature, meaning that key objects on the K4 will be zeroized.

The table below lists those capabilities that are supported on the Cavium K4, including whether they are allowed as a part of the standard (default) configuration, the ability of the SO to enable/disable the capability as a matter of policy, and the destructive nature of the policy change.

Table C-1 Security Related Capabilities Supported on the Cavium K4 Cryptographic Module HSM

Capability	Default Configuration	Policy Change [1]	Description
Non-FIPS Algorithms	Yes	Enabled/Destructive	This capability allows non-FIPS algorithms to be executed on the K4. The SO may disable this capability but this action will destroy all key material existing on the HSM.
Activation	Yes	Disabled/ Non-destructive	This capability allows for FIPS level 3 User authentication with the challenge-response password only, after initial login with the User black PED key. For more details refer to Authentication Modes section.
Auto-Activation	Yes	Disabled/Non-destructive	This capability allows for FIPS level 3 User authentication with the challenge-response password only, after an initial login with the User black PED key, and a short-duration power loss to the K4.
Change Attributes	Yes	Enabled/Non-destructive	This capability allows key attributes to be changed.
Private Key Wrapping	No (Cannot be allowed with SIM support)	Disabled/Destructive	This capability allows the wrapping (extraction) of private keys from the K4. This capability is generally considered to compromise the security of the private key, and is only advised where use of the private key is required in software. In that case a PBE derived wrapping key can be created both in software and on the K4. For off-board key storage or replication of keys across multiple HSMs, the Secure Information Management (SIM) capability is a more secure solution (see below).
SIM	Yes	Disabled/Destructive	SIM is a capability whereby a special SIM Masking key (created at initialization) is used to wrap (encrypt) private key objects for off-board storage or replication of keys across multiple K4s (see also HSM-Cloning).
HSM-Cloning	Yes	Disabled/Destructive	HSM-Cloning provides the capability of replicating the SIM Masking key across multiple HSMs. This capability would be required if operations require that private keys are replicated across multiple K4s.
Secret Key Wrapping	Yes	Disabled/Destructive	This capability allows for the wrapping of secret keys.

Note 1: This column indicates the default policy setting, and whether any change to the policy by the SO is destructive.

APPENDIX D. LIST OF TERMS, ABBREVIATIONS AND ACRONYMS

Term	Definition
CA	Certification Authority
Chrysalis-ITS	Former name of SafeNet Canada, Inc.
DAK	Device Authentication Key
FIPS	Federal Information Processing Standard
GSK	Global Storage Key
HA	High Availability
HOK	Hardware Origin Key
HSM	Hardware Security Module
MVK	Manufacturers Verification Key
PCI	Peripheral Component Interconnect
PED	PIN Entry Device
SCU	Secure Capability Update
SGSK	Secondary Global Storage Key
SIM	Secure Information Management
SMK	Security Officer’s Master Key
SO	Security Officer
TSK	Token or K4 Signing Key
TVK	Token or K4 Variable Key
TWK	Token or K4 Wrapping Key
USK	User’s Storage Key