VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304, USA
Tel: 877-486-9273
Email: info@vmware.com
http://www.vmware.com

VMware's SD-WAN VPN Hybrid Crypto Module

Hardware Versions: Intel Atom C3308, Intel Atom C3558, Intel Atom C3958 and Intel Xeon D-2187NT

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.0

TABLE OF CONTENTS

List of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VMware's SD-WAN VPN Hybrid Crypto Module from VMware, Inc. This Security Policy describes how the VMware's SD-WAN VPN Hybrid Crypto Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The VMware's SD-WAN VPN Hybrid Crypto Module is also referred to in this document as “the module”.

1.2 Reference

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The VMware website (http://www.vmware.com) contains information on the full line of products from VMware.
- The CMVP website (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search) contains options to get contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to VMware and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact VMware, Inc.

2 VMware's SD-WAN VPN Hybrid Crypto Module

2.1 Introduction

VMware, Inc., a global leader in virtualization, cloud infrastructure, and business mobility, delivers customer-proven solutions that accelerate Information Technology (IT) by reducing complexity and enabling more flexible, agile service delivery. With VMware solutions, organizations are creating exceptional experiences by mobilizing everything, responding faster to opportunities with modern data and apps hosted across hybrid clouds, and safeguarding customer trust with a defense-in-depth approach to cybersecurity. VMware enables enterprises to adopt an IT model that addresses their unique business challenges. VMware's approach accelerates the transition to solutional-computing while preserving existing investments and improving security and control.

2.2 Cryptographic Module Specification

VMware's SD-WAN VPN Hybrid Crypto Module is a software-hybrid cryptographic module whose purpose is to provide FIPS 140-2 validated cryptographic functions to various VMware applications utilizing VPN capabilities.

The Module is defined as a multi-chip standalone cryptographic module and has been validated at the FIPS 140-2 overall Security Level 1. Table 1 below describes the level achieved by the module in each of the eleven sections of the FIPS 140-2 requirements.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[1]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

[1] EMI/EMC – Electromagnetic Interference/Electromagnetic Compatibility

The FIPS 140-2 operational testing was performed on the configurations presented in Table 2.

Table 2 – Tested Configurations

Operating System	Processor	Acceleration	Hardware Platform
VMware SD-WAN OS 4.0	Intel© Atom C3308	Intel© QAT[2]	VMware SD-WAN Edge 610
VMware SD-WAN OS 4.0	Intel© Atom C3558	Intel© QAT	VMware SD-WAN Edge 620
VMware SD-WAN OS 4.0	Intel© Atom C3958	Intel© QAT	VMware SD-WAN Edge 680
VMware SD-WAN OS 4.0	Intel©Xeon D-2187NT	Intel© QAT	VMware SD-WAN Edge 3810

Because the VMware's SD-WAN VPN Hybrid Crypto Module is defined as a software-hybrid cryptographic module, it possesses both a physical cryptographic boundary and a logical cryptographic boundary.

[2] QAT – QuickAssist Technology

2.2.1 Physical Cryptographic Boundary

As a software-hybrid module, the module must rely on the physical characteristics of the host systems i.e. the VMware Edge devices. The physical boundary of the cryptographic module is defined by the hard enclosure around the host systems on which it runs. The host systems consist of integrated circuits of the system board, processor, RAM, hard disk, device case and power supply. See Figure 1 below for a block diagram of the host system.

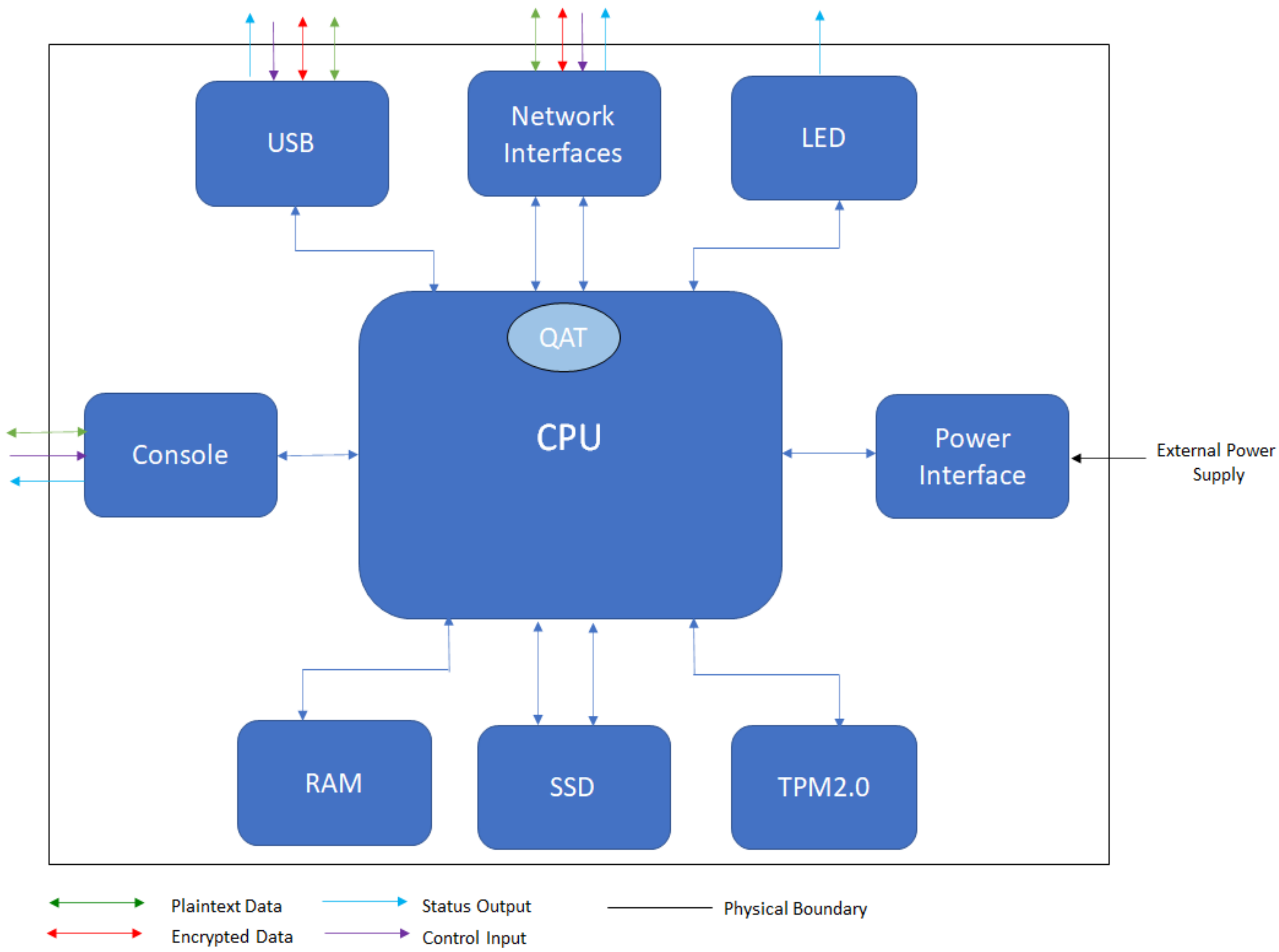

Figure 1 – Hardware Block Diagram

Figure 2 – Intel Processors (Hardware Component)

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary for the VMware's SD-WAN VPN Hybrid Crypto Module is depicted in Figure 3. The VMware's SD-WAN VPN Hybrid Crypto Module boundary consists of three object files, librte_cryptodev.so, libcrypto_post.so and librte_pmd_qat.so. The libcrypto_post.so is responsible for performing the integrity testing and all power-on self-tests, and librte_cryptodev.so provides cryptographic services to the application components once the integrity tests and power-on self-tests have passed successfully.

The colored arrows, in Figure 3, indicate the logical information flows into and out of the module.

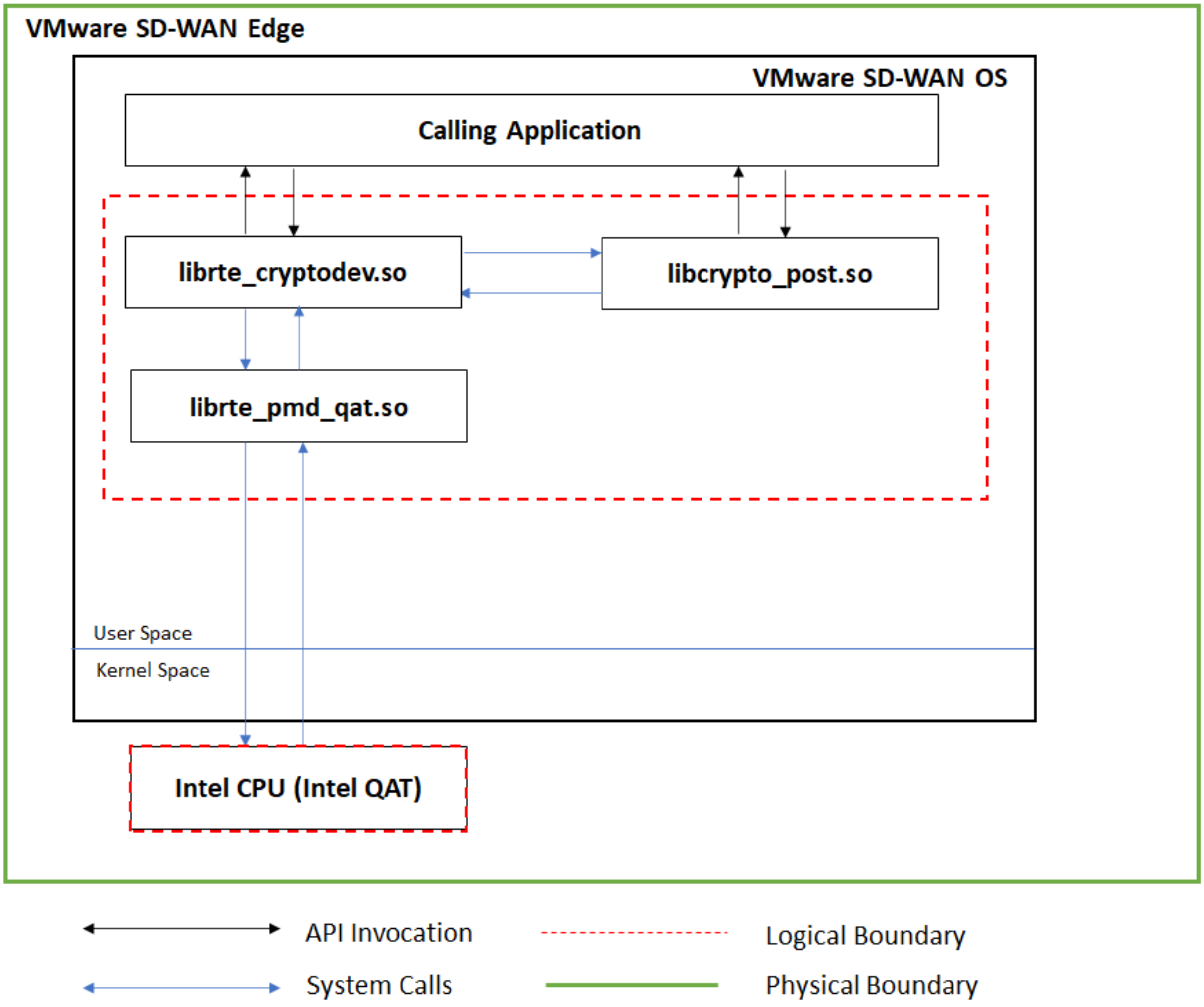

Figure 3 – Module's Logical Cryptographic Boundary

2.2.3 Modes of Operation

The VMware's SD-WAN VPN Hybrid Crypto Module only supports a FIPS-Approved mode of operation. The module must be configured as described in section 3.

Table 3 includes the FIPS-Approved algorithms.

Table 3 – FIPS-Approved Algorithms

Algorithm	Modes	Certificate Number
AES (128 and 256-bit keys)	CBC, GCM	#C1813
SHS	SHA-1, SHA-256, SHA-384, and SHA-512	#C1813
HMAC	SHA-1, SHA-256, SHA-384, and SHA-512	#C1813

2.3 Module Interfaces

The module's logical interfaces exist at a low level in the software as an API. Both the API and physical interfaces can be categorized into the following interfaces defined by FIPS 140-2:

- Data input
- Data output
- Control input
- Status output
- Power input

As a software-hybrid module, the module's manual controls, physical indicators, and physical and electrical characteristics are those of the host platform. A mapping of the FIPS 140-2 defined interfaces and the logical interfaces of the module can be found in Table 4 below.

Table 4 – FIPS 140-2 Logical Interface Mapping

FIPS Interface	Logical Interface	Physical Interface
Data Input	The function calls that accept input data for processing through their arguments.	Network ports, serial port, USB ports
Data Output	The function calls that return by means of their return codes or argument generated or processed data back to the caller.	Network ports, serial port, USB ports
Control Input	The function calls that are used to initialize and control the operation of the module.	Network ports, serial port, USB ports, Power button
Status Output	Return values for function calls; Module generated error messages.	Network ports, serial port, USB ports, LED
Power Input	Not applicable.	AC power socket

2.4 Roles, Services and Authentication

2.4.1 Roles

There are two roles in the module (as required by FIPS 140-2) that operators may assume: A Crypto-Officer (CO) role and a User role. Each role and their corresponding services are detailed in the sections below. The User and Crypto-Officer roles are implicitly assumed by the entity accessing the module services. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 5 below indicate the types of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an FIPS-Approved or Allowed security function or authentication mechanism.

2.4.2 Services

Table 5 below describes the CO and User services.

Table 5 – Crypto Officer and User Services

Role	Service	Description	CSP and Type of Access
CO, User	Encryption	Encrypt plaintext using supplied key and algorithm specification	AES Key (CBC, GCM) – RX AES GCM IV – RX
CO, User	Decryption	Decrypt ciphertext using supplied key and algorithm specification	AES Key (CBC, GCM) – RX AES GCM IV – RX
CO, User	Hashing	Compute and return a message digest using SHA algorithm	None
CO, User	Message Authentication Code generation	Compute and return a hashed message authentication code	HMAC Key – RX
CO, User	Show Status	Show current operational mode of the module	None
CO, User	Run On-Demand Self-Tests	Execute required self-tests	AES Key (CBC, GCM) – RX AES GCM IV – RX HMAC Key – RX
CO, User	Key Zeroization	Zeroize all Keys and CSP	AES Key (CBC, GCM) – W AES GCM IV – W HMAC Key – W

2.4.3 Authentication

The module is a Level 1 software-hybrid cryptographic module and does not implement authentication. Roles are assumed implicitly through the execution of either a CO or a User service.

2.5 Physical Security

The VMware's SD-WAN VPN Crypto Module is a software-hybrid module, which FIPS 140-2 defines as a multi-chip standalone cryptographic module. The physical cryptographic boundary is the hard enclosure around the host platform on which it runs. All physical components are made of production-grade materials, and all integrated circuits (ICs) in the module are coated with commercial standard passivation.

2.6 Operational Environment

The module was tested and found to be compliant with FIPS 140-2 requirements on the Operational Environments listed in Table 2.

The module has been confirmed by the vendor to be operational on the following platforms. As allowed by the FIPS 140-2 Implementation Guidance G.5, the validation status of the Cryptographic Module is maintained when operated in the following additional operating environments:

- VMware SD-WAN Edge 510
- VMware SD-WAN Edge 510-LTE-APAC
- VMware SD-WAN Edge 510-LTE-NAM-EMEA
- VMware SD-WAN Edge 520
- VMware SD-WAN Edge 520v
- VMware SD-WAN Edge 540
- VMware SD-WAN Edge 610-LTE-AE
- VMware SD-WAN Edge 610-LTE-RW
- VMware SD-WAN Edge 640
- VMware SD-WAN Edge 840
- VMware SD-WAN Edge 2000
- VMware SD-WAN Edge 3400
- VMware SD-WAN Edge 3800
- A General-Purpose Computer (GPC) with a processor implementing Intel© QAT
- VMware SD-WAN Virtual Edge

Further, VMware affirms that the module maintains compliance to FIPS 140-2 when ported together to other Edge devices or platforms (including GPCs) using Intel© processors comprising of the Intel QAT provided the module software component is unmodified i.e. no source code modifications are made, hardware components utilized by the controlling software is not modified, and the same operating system (i.e. same version number) as specified on the validation certificate is used. The CMVP allows porting of the validated hybrid cryptographic module from the operational environment specified on the validation certificate to a new operational environment as long as the porting rules are followed.

No claim can be made as to the correct operation of the module when the module is ported to an operational environment that is not listed on the CMVP validation certificate.

All cryptographic keys and CSPs are under the control of the OS, which protects its CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined API.

The tested operating system segregates user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the calling application, and implicitly satisfies the FIPS 140-2 requirement for a single user mode of operation.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 6.

Table 6 – List of Cryptographic Keys, Key Components, and CSPs

Key/CSP	Key/CSP Description	Generation/Input	Output	Storage	Zeroization	Use
AES Key	128 and256-bit key	Input via API in plaintext	None	In RAM	Reboot OS; Cycle host power	Encryption, Decryption
AES GCM Key	128 and256-bit key	Input via API in plaintext	None	In RAM	Reboot OS; Cycle host power	Encryption, Decryption
AES GCM IV	96-bit	Input via API in plaintext	None	In RAM	Reboot OS; Cycle host power	Encryption, Decryption
HMAC Key	112-bit key	Input via API in plaintext	None	In RAM	Reboot OS; Cycle host power	Message Authentication

2.7.1 Key Generation

The Module does not implement any random number generator for the generation of random bits or keys. The cryptographic module is passed keys and CSPs as API parameters, associated by memory location. The application calling the cryptographic module passes keys and CSPs in plaintext within the physical boundary.

2.7.2 Key Entry/Output

Symmetric keys are provided to the module by the calling process and are destroyed when released by the appropriate API function calls. The module does not perform persistent storage of keys.

2.7.3 Zeroization

Keys and CSPs can be zeroized by rebooting the host hardware platform.

2.8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The VMware Edge hardware platforms listed in Table 2 have been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at their own expense.

2.9 Self-Tests

Cryptographic self-tests are performed by the module after initialization of the module, and on demand by power cycling the module. The module does not implement any algorithms that require conditional self-tests. The following sections list the self-tests performed by the module, their expected error status, and any error resolutions.

Self-tests are health checks that ensure the cryptographic algorithms implemented within the module are operating correctly. The self-tests identified in FIPS 140-2 broadly fall within two categories:

1. Power-On Self-Tests
2. Conditional Self-Tests

2.9.1 Power-On Self-Tests

The module performs the required set of power-on self-tests. These self-tests are performed automatically by the module when the module is powered-up. The list of power-on self-tests that follows may also be run on-demand when the CO reboots the Operating System. The module will perform the listed power-on self-tests to successful completion. During the execution of self-tests, data output from the module is inhibited.

If any of the self-tests fail, the module will return an error code to the application that tried to load and initialize the module. The module will enter an error state and none of the module's services are available in the error state. In order to resolve a cryptographic self-test error, the module must be restarted by rebooting the OS. If the error persists, the software must be reinstalled.

The VMware's SD-WAN VPN Hybrid Crypto Module performs the following Power-On Self-Tests:

- Software integrity check
  - HMAC SHA-256

- Known Answer Tests (KATs)
  - AES CBC Encryption KAT (128 and 256-bit)
  - AES CBC Decryption KAT (128 and 256-bit)
  - AES GCM Encryption KAT (128 and 256-bit)
  - AES GCM Decryption KAT (128 and 256-bit)
  - HMAC SHA-1, HMAC SHA-256, HMAC-SHA-384 and HMAC SHA-512 KAT (also test SHA-1, SHA-256, SHA-384 and SHA-512)

2.9.2 Conditional Self-Tests

The module does not implement any algorithm that requires the module to perform any conditional self-tests.

2.10 Mitigation of Other Attacks

This section is not applicable. The module was not designed to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The VMware's SD-WAN VPN Hybrid Crypto Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-Approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 VMware's VPN Hybrid Crypto Module Secure Operation

There are no additional steps beyond powering on the device that must be performed to use the module correctly.

3.2 User Guidance

The User or API functions calls should be designed to deal with the identified error cases of the VMware's SD-WAN VPN Hybrid Crypto Module.

Per IG A.5 the AES GCM IV is constructed in compliance with the IPsec-v3 protocol per RFC 4106 and is to be used in the context of the AES GCM mode encryption within the IPsec-v3 protocol alone.

The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. Per requirements of IPSec-v3, the IV constitutes of 32-bits of salt followed by 64-bits of deterministic nonce. The last 64 bits of the IV are deterministically constructed using an incremental counter. In the event that the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established. When the nonce portion of the IV exhausts the maximum number of possible values for a given security association, either party to the security association that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key for the security association per RFC 7296.

There are no additional user guidance instructions for the correct operation of the module.

4 ACRONYMS

Table 7 provides definitions for the acronyms used in this document.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FCC	Federal Communications Commission
GCM	Galois/Counter Mode
HMAC	(Keyed) Hash Message Authenticating Code
IT	Information Technology
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
VPN	Virtual Private Network