Arista Networks, Inc.

Arista MACsec data plane accelerator [PHY]

Version: v1.0

FIPS 140-3 Non-Proprietary Security Policy

Document prepared by:

http://www.lightshipsec.com

2025 Arista Networks, Inc. and Lightship Security, Inc.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Table of Contents

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

List of Tables

List of Figures

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

1 General

1.1 Overview

This non-proprietary FIPS 140-3 Security Policy for the Arista MACsec data plane accelerator [PHY], version v1.0 describes how the module meets the security requirements specified in FIPS 140-3 for an overall security level 1 module and outlines the security rules and operating procedures required to maintain compliance.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

Arista MACsec encryption is used by networking infrastructure to secure traffic across cloud networks consisting of long-distance and large-scale data communications across the globe and is protected by strong cryptography that meets regulatory requirements.

Module Type: Software-hybrid

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the Arista MACsec data plane accelerator [PHY] consists of a hardware and a software component, which is represented by the red dash line in Figure 5, below. The physical perimeter of the module is defined as the entire MACsec PHY. The sole software component of the module consists of the entire module's software, which is contained in libMacsecFipsExt.so.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Tested Operational Environment's Physical Perimeter (TOEPP):

The single chips shown below represent the entire physical perimeter of the module itself and implement the core cryptographic functionality of the module, AES-GCM encryption and decryption (with extended packet numbering) used within the MACsec protocol. The Tested Operational Environment's Physical Perimeter consists of the Arista network devices that the module resides within. The tested operational environments are listed in Table *Tested Operational Environments - Software, Firmware, Hybrid*, below.

Figure 1: Credo CMS42550 physical perimeter.

Figure 2: Credo CMR52241 physical perimeter.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Figure 3: Credo CMS50216 physical perimeter.

Figure 4: Credo CMR55321 physical perimeter.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

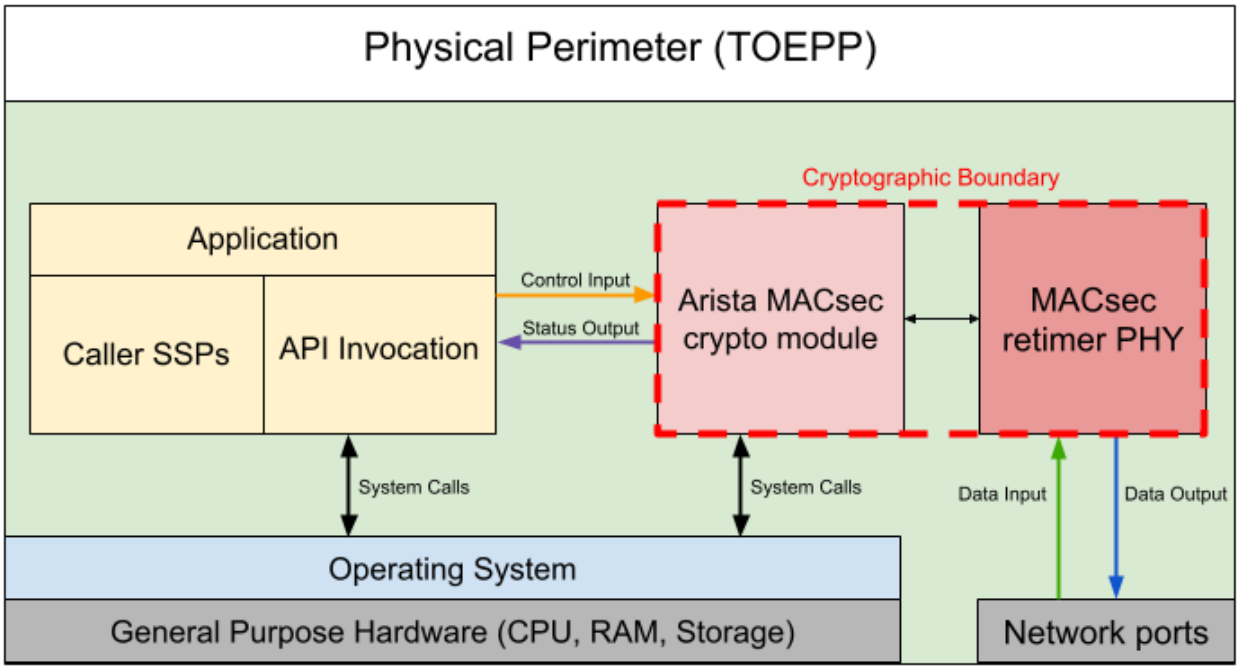

Figure 5: Module cryptographic boundary and TOEPP.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
libMacsecFipsExt.so	v1.0	Shared Library, Contains entire module's software	SHA3-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
CMS42550	rev B0	owl.lz4.fw.1.94.11.B0.bin	CMS42550 rev B0	Single chip
CMR52241	rev B0	osprey.lz4.fw.1.0.10.bin	CMR52241 rev B0	Single chip
CMS50216	rev B0	owl.lz4.fw.1.94.11.B0.bin	CMS50216 rev B0	Single chip
CMR55321	rev B0	osprey.lz4.fw.1.0.10.bin	CMR55321 rev B0	Single chip

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Arista EOSv4	Arista DCS-7050CX4M-48D8	AMD Ryzen™ Embedded V1500B	No	-	v1.0
Arista EOSv4	Arista DCS-7050DX4M-32S	AMD EPYC™ Embedded 3151	No	-	v1.0
Arista EOSv4	Arista 7388 with 7388-SUP-D (Supervisor containing main CPU) and 7388-8D (Line card containing PHY)	Intel® Xeon® Processor D-1527	No	-	v1.0
Arista EOSv4	Arista DCS-7804-CH with DCS-7800-SUP1A (Supervisor containing main CPU) and 7800R3-48CQM2-LC (Line card containing PHY)	Intel® Xeon® Processor D-1528	No	-	v1.0

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform
Arista EOSv4	DCS-7170B-64C
Arista EOSv4	DCS-7280CR3MK-32D4
Arista EOSv4	DCS-7280CR3MK-32D4A-S
Arista EOSv4	DCS-7280CR3MK-32D4S
Arista EOSv4	DCS-7280CR3MK-32P4
Arista EOSv4	DCS-7280CR3MK-32P4S
Arista EOSv4	DCS-7800R3-48CQMS-LC
Arista EOSv4	DCS-7800R3K-36DM-LC

Table 5: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

There are no module components excluded from the validation.

2.4 Modes of Operation

Modes List and Description:

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Mode Name	Description	Type	Status Indicator
Approved mode	The approved mode of operation	Approved	Log ("selfTestsSucceeded")

Table 6: Modes List and Description

Once these self-tests have completed successfully, the module transitions into the approved mode of operation. There are no other modes of operation implemented by the module.

2.5 Algorithms

Approved Algorithms:

Credo Owl

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A1359	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A1359	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D
AES-XPN	A1359	Direction - Decrypt, Encrypt Key Length - 128, 256 IV Generation - External	SP 800-38D

Table 7: Approved Algorithms - Credo Owl

Credo Osprey

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A1902	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A1902	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D
AES-XPN	A1902	Direction - Decrypt, Encrypt Key Length - 128, 256 IV Generation - External	SP 800-38D

Table 8: Approved Algorithms - Credo Osprey

SHA3 Implementation

Algorithm	CAVP Cert	Properties	Reference
SHA3-256	A7380	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 202

Table 9: Approved Algorithms - SHA3 Implementation

The Approved Algorithms tables above list the approved algorithms implemented by the Arista MACsec data plane accelerator [PHY].

Vendor-Affirmed Algorithms:

The module does not implement any vendor-affirmed algorithms.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Non-Approved, Allowed Algorithms:

The module does not implement any non-approved, allowed algorithms.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not implement any non-approved, allowed algorithms with no security claimed.

Non-Approved, Not Allowed Algorithms:

The module does not implement any non-approved, not allowed algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encrypt Data	BC-Auth	Encryption of data in MACsec protocol	Publication:NIST SP 800-38D IG:C.H	AES-ECB: (A1359, A1902) AES-GCM: (A1359, A1902) AES-XPN: (A1359, A1902)
Decrypt Data	BC-Auth	Encryption of data in MACsec protocol	Publication:NIST SP 800-38D IG:C.H	AES-ECB: (A1359, A1902) AES-GCM: (A1359, A1902) AES-XPN: (A1359, A1902)
Software/Firmware Integrity Test	SHA	Integrity test for chip firmware and module software		SHA3-256: (A7380)

Table 10: Security Function Implementations

2.7 Algorithm Specific Information

The AES-GCM Initialization Vector (IV) generation is compliant with IG C.H, resolution 1(c). The module generates IVs deterministically following the guidance in IEEE 802.1AE.

While operating the approved mode of operation, the module should only be used to form a MACsec link with another FIPS 140 validated module operating in the approved mode. The device on each end of the MACsec link plays the role of either the Peer or the Authenticator. No authentication server is involved.

In case the module's power is lost and then restored, the key used for AES-GCM encryption and decryption operations shall be redistributed.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

2.8 RBG and Entropy

SSPs used in the module are generated outside the module, deterministically, in accordance with the MACsec protocol. The module itself does not generate any SSPs. Therefore, the module does not implement a DRBG and does not require an entropy source.

2.9 Key Generation

The module only generates the AES-GCM Initialization Vector deterministically, following the guidance given in IG C.H (path 1, c) and IEEE 802.1AE.

2.10 Key Establishment

The module does not implement any key establishment schemes.

2.11 Industry Protocols

The module itself does not implement any industry protocols protocol.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Serdes A0-A7	Data Input	Plaintext data to be encrypted, Encrypted data to be decrypted
Serdes B0-B7	Data Output	Plaintext data that has been decrypted, Encrypted data that has been encrypted, AES-GCM IV to the calling application
N/A	Data Input	The module accepts data input (cryptographic keys) through the input arguments of the API functions
N/A	Control Input	The module accepts control input through the input arguments of the API functions used to control the module
N/A	Status Output	The module produces status output through the return values from function calls and error messages.
VDD, VDD_IO, VAA_AGC, VAA, GND	Power	Electrical power to the module

Table 11: Ports and Interfaces

The Ports and Interfaces table above specifies the cryptographic module interfaces. The physical interfaces are defined as the data input/output pins of the MACsec chips. The logical interfaces are logically separated from one another by the hybrid module design. The power interface is physically separate from the other physical interfaces as the voltage pins are distinct from the data input/output pins of the chips. The module does not implement a control output interface.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not implement any authentication mechanisms. The sole role (Crypto Officer) is assumed implicitly.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 12: Roles

The module supports the Crypto Officer role only. This sole role is implicitly assumed by the operator of the module when performing a service.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Output approved mode status	Global (completion of service)	Command	Status Output (return code = true)	None	Crypto Officer
Show Module's Versioning Information	Output the module name and version identifiers	Global (completion of service)	Command	Status Output ("Arista MACsec data plane accelerator [PHY] v1.0")	None	Crypto Officer
Perform Self-tests	Runs the software/firmware integrity check and cryptographic algorithm self tests on demand	Global (completion of service)	Command/Procedure	Status Output (pass/fail)	Encrypt Data Decrypt Data Software/Firmware Integrity Test	Crypto Officer

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform Zeroisation	Zeroise SSPs stored temporarily in RAM and in the chip registers	Global (completion of service)	Command/Procedure	Status Output	None	Crypto Officer - AES-GCM Key: Z - AES-GCM IV: Z
Encrypt Data	Encrypt plaintext data	Global (completion of service)	Plaintext Data (Network Traffic)	Encrypted Data (Network Traffic)	Encrypt Data	Crypto Officer - AES-GCM Key: W,E - AES-GCM IV: G,E
Decrypt Data	Decrypt ciphertext data	Global (completion of service)	Encrypted Data (Network Traffic)	Plaintext Data (Network Traffic)	Decrypt Data	Crypto Officer - AES-GCM Key: W,E - AES-GCM IV: G,E

Table 13: Approved Services

The module provides approved services to the operator who assumes the Crypto Officer role as defined in this document.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

The approved services defined in this section implement the security function implementations defined in section 2.6 of this document.

4.4 Non-Approved Services

The module does not implement any non-approved services.

4.5 External Software/Firmware Loaded

The module does not perform loading of any code from an external source.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The approved integrity technique is implemented by the cryptographic module itself. The approved software and firmware integrity technique consists of 2 self-tests, run pre-operationally.

Software component integrity test:

The module software component (libMacsecFipsExt.so) is covered with an approved integrity technique (SHA3-256) which is implemented in the module software. If the calculated integrity value does not match the reference value embedded into the software, the module enters the Hard Error state and terminates execution of module.

PHY firmware integrity test:

The PHY's firmware (owl.lz4.fw.1.94.11.B0.bin for CMS42550 and CMS50216, osprey.lz4.fw.1.0.10.bin for CMR52241 and CMR55321) are covered with the same approved integrity technique (SHA3-256) which is used by the Software integrity test. If the calculated integrity value of the PHY memory containing the firmware does not match the reference value embedded into the module software, the module enters the Soft Error state and the PHY become non-operational and will not respond to cryptographic service requests.

5.2 Initiate on Demand

The conditional algorithm self-tests are run at module startup in addition to the firmware integrity test. The crypto officer can initiate the self-tests on demand by power-cycling the host platform (TOEPP).

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

The Crypto Officer should confirm that the module is operating in the approved mode by checking for the approved mode indicator per the instructions in Section 11.2 of this document.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

7 Physical Security

Each module's hardware consists of a single chip made with production grade components, protected by a conformal coating as a standard passivation technique. As the software portion of the hybrid module execute within a limited operational environment, the module is defined as a multi-chip standalone embodiment.

The module itself provides no additional physical security techniques. However, the module will reside inside of an Arista device which is installed within a secure Arista facility. The module will therefore inherit these additional physical characteristics and protections.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

8 Non-Invasive Security

The module does not implement any security mechanisms which protect against non-invasive attacks.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Volatile Memory	Stored temporarily in memory within MACsec module.	Dynamic
External	Stored temporarily in memory location associated with the calling application.	Dynamic

Table 14: Storage Areas

The module stores keys and input/output data temporarily in volatile memory. The module does not store keys or data persistently.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SSP Input (GCM encrypt)	External	Volatile Memory	Plaintext	Automated	Electronic	Encrypt Data
SSP Input (GCM decrypt)	External	Volatile Memory	Plaintext	Automated	Electronic	Decrypt Data
IV Output (GCM encrypt)	Volatile Memory	External	Plaintext	Automated	Electronic	Encrypt Data
IV Input (GCM decrypt)	External	Volatile Memory	Plaintext	Automated	Electronic	Decrypt Data

Table 15: SSP Input-Output Methods

SSPs are only input from the calling applications within the module's TOEPP. This method is categorized as automated distribution, electronic entry ("CM Software from App via TOEPP Path").

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Remove Power	Remove power from the host platform	Keys are procedurally zeroized by rebooting the host platform, which is acceptable at Software level 1.	Crypto Officer reboots or removed power from host platform

Table 16: SSP Zeroization Methods

SSPs are zeroised procedurally by power-cycling the host platform.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

9.4 SSPs

The following table summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES-GCM Key	Encryption and Decryption	128 or 256 bits - 128 or 256 bits	Authenticated Symmetric Key - CSP			Encrypt Data Decrypt Data
AES-GCM IV	Initialization Vector for AES-GCM MACsec encryption	96 bits - N/A	Initialization Vector - CSP	Encrypt Data Decrypt Data		Encrypt Data Decrypt Data

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-GCM Key	SSP Input (GCM encrypt) SSP Input (GCM decrypt)	Volatile Memory:Plaintext	Until zeroised	Remove Power	AES-GCM IV:Used With
AES-GCM IV	IV Output (GCM encrypt) IV Input (GCM decrypt)	Volatile Memory:Plaintext	Until zeroised	Remove Power	AES-GCM Key:Used With

Table 18: SSP Table 2

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA3-256 (A7380)	SHA3-256	KAT	SW/FW Integrity	Log entry: "MacsecFipsExt integrity check passed" OR "MacsecFipsExt integrity check failed"	Software component Integrity test using an approved hash (SHA3)
SHA3-256 (A7380)	SHA3-256	KAT	SW/FW Integrity	Log Entry: "Firmware integrity finished with result: <true / false>"	Integrity test with SHA3-256 over PHY memory containing firmware

Table 19: Pre-Operational Self-Tests

The module's startup integrity test is performed upon the module.

As the modules do not implement bypass capability or any FIPS-defined critical functions, no additional pre-operational self-tests are required.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-256 (A7380)	SHA3-256	KAT	CAST	"Self-test failed for integrity test algorithm"	Compare calculated hash to pre-loaded hash result	Before running of the SW/FW Integrity Test. / Immediately when the module enters the approved mode of operation.
AES-XPN (A1359)	128 bits	KAT	CAST	'Ethernet<x/y>': POST complete	Encrypt (using extended packet numbering function), Credo 'Owl' PHYs	Before first operational use of encryption service. / Immediately when the module enters the approved

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						mode of operation.
AES-XPN Decrypt (A1359)	128 bits	KAT	CAST	'Ethernet<x/y>': POST complete	Decrypt (using extended packet numbering function), Credo 'Owl' PHYs	Before first operational use of decryption service. / Immediately when the module enters the approved mode of operation.
AES-XPN (A1902)	128 bits	KAT	CAST	'Ethernet<x/y>': POST complete	Encrypt (using extended packet numbering function), Credo 'Osprey' PHYs	Before first operational use of encryption service. / Immediately when the module enters the approved mode of operation.
AES-XPN Decrypt (A1902)	128 bits	KAT	CAST	'Ethernet<x/y>': POST complete	Decrypt (using extended packet numbering function), Credo 'Osprey' PHYs	Before first operational use of decryption service. / Immediately when the module enters the approved mode of operation.

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-256 (A7380)	KAT	SW/FW Integrity	Upon module startup	Manual (reboot host platform)
SHA3-256 (A7380)	KAT	SW/FW Integrity	Upon module startup	Manual (reboot host platform)

Table 21: Pre-Operational Periodic Information

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-256 (A7380)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
AES-XPN (A1359)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
AES-XPN Decrypt (A1359)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
AES-XPN (A1902)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
AES-XPN Decrypt (A1902)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device

Table 22: Conditional Periodic Information

The operator can perform the pre-operational and conditional self-tests on demand by power-cycling the host platform.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Hard Error	Module does terminated operation, Host device must be restarted	Module fails SHA3 CAST, or Software Integrity Test	Reboot host platform	Module terminates operation
Soft Error	PHY is non-operational and will not respond to service requests.	Module fails firmware integrity check, or XPN CAST for the PHY	Reboot host platform	return code = false

Table 23: Error States

When the module fails the SHA3-256 CAST or the Software Component Integrity Test, the module will immediately print a self-test failure indicator to the device log and proceed to the Hard Error state. When in the Hard Error state, the module will terminate execution completely and therefore, all cryptographic operation is inhibited.

When the module fails the Firmware Integrity Check, or AES-XPN CASTs, the module will immediately print a self-test failure indicator to the device log and proceed to the Soft Error state. When in the Soft Error state, the PHY becomes non-operational and will not respond to service requests and therefore, all cryptographic operation is inhibited.

10.5 Operator Initiation of Self-Tests

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

The operator can perform the conditional self-tests on demand by power-cycling the host platform.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Arista MACsec data plane accelerator [PHY] is pre-installed and configured at an Arista facility and offered to end users as an integrated part of Arista's service offerings. As such, there are no installation, initialization, or startup procedures to be performed by the Crypto Officer.

11.2 Administrator Guidance

The Crypto Officer should ensure that the module is running in the approved mode of operation before use. This can be determined by checking the device log to confirm the output of the 'Show Module's Versioning Information' and 'Show Status' services as listed in the 'Approved Services' section of this document.

11.3 Non-Administrator Guidance

In case the module's power is lost and then restored, the key used for MACsec encryption and decryption shall be redistributed.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

The module does not implement any security mechanisms which protect against other attacks.

This document may be freely reproduced and distributed whole and intact, including this copyright notice.