Arista Networks, Inc.

Arista MACsec data plane accelerator [on-chip-driver]

Version: 1.0

FIPS 140-3 Non-Proprietary Security Policy

Document prepared by:

http://www.lightshipsec.com

Table of Contents

1.1 Overview 6
1.2 Security Levels 6
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 9
2.3 Excluded Components 10
2.4 Modes of Operation 10
2.5 Algorithms 10
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 13
2.8 RBG and Entropy 13
2.9 Key Generation 13
2.10 Key Establishment 13
2.11 Industry Protocols 13
3 Cryptographic Module Interfaces 14
3.1 Ports and Interfaces 14
4 Roles, Services, and Authentication 15
4.1 Authentication Methods 15
4.2 Roles 15
4.3 Approved Services 15
4.4 Non-Approved Services 17
4.5 External Software/Firmware Loaded 17
5 Software/Firmware Security 18
5.1 Integrity Techniques 18
5.2 Initiate on Demand 18
6 Operational Environment 19
6.1 Operational Environment Type and Requirements 19
7 Physical Security 20
8 Non-Invasive Security 21
9 Sensitive Security Parameters Management 22
9.1 Storage Areas 22
9.2 SSP Input-Output Methods 22
9.3 SSP Zeroization Methods 22
9.4 SSPs 23
10 Self-Tests 24

10.1 Pre-Operational Self-Tests 24
10.2 Conditional Self-Tests 24
10.3 Periodic Self-Test Information 25
10.4 Error States 25
10.5 Operator Initiation of Self-Tests 26
11 Life-Cycle Assurance 27
11.1 Installation, Initialization, and Startup Procedures 27
11.2 Administrator Guidance 27
11.3 Non-Administrator Guidance 27
11.4 Additional Information 27
12 Mitigation of Other Attacks 28

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 9
Table 3: Tested Module Identification – Hybrid Disjoint Hardware 9
Table 4: Tested Operational Environments - Software, Firmware, Hybrid 10
Table 5: Modes List and Description 10
Table 6: Approved Algorithms - Q3D (BCM88870) 11
Table 7: Approved Algorithms - JC2+ (BCM88850) 11
Table 8: Approved Algorithms - Integrity Test Library 12
Table 9: Security Function Implementations 12
Table 10: Ports and Interfaces 14
Table 11: Roles 15
Table 12: Approved Services 17
Table 13: Storage Areas 22
Table 14: SSP Input-Output Methods 22
Table 15: SSP Zeroization Methods 22
Table 16: SSP Table 1 23
Table 17: SSP Table 2 23
Table 18: Pre-Operational Self-Tests 24
Table 19: Conditional Self-Tests 25
Table 20: Pre-Operational Periodic Information 25
Table 21: Conditional Periodic Information 25
Table 22: Error States 25

List of Figures

Table 1: Security Levels 6
Figure 1: Broadcom BCM88850 physical perimeter. 7
Figure 2: Arista DCS-7800R3AK-36DM2-LC line card (TOEPP) 7
Figure 3: Broadcom BCM88870 physical perimeter. 8
Figure 4: Arista DCS-7280R4K-32DE switch (TOEPP) 8
Figure 5: Module cryptographic boundary and TOEPP. 8
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 9
Table 3: Tested Module Identification – Hybrid Disjoint Hardware 9
Table 4: Tested Operational Environments - Software, Firmware, Hybrid 10
Table 5: Modes List and Description 10
Table 6: Approved Algorithms - Q3D (BCM88870) 11
Table 7: Approved Algorithms - JC2+ (BCM88850) 11
Table 8: Approved Algorithms - Integrity Test Library 12
Table 9: Security Function Implementations 12
Table 10: Ports and Interfaces 14
Table 11: Roles 15
Table 12: Approved Services 17
Table 13: Storage Areas 22
Table 14: SSP Input-Output Methods 22
Table 15: SSP Zeroization Methods 22
Table 16: SSP Table 1 23
Table 17: SSP Table 2 23

Table 18: Pre-Operational Self-Tests 24
Table 19: Conditional Self-Tests 25
Table 20: Pre-Operational Periodic Information 25
Table 21: Conditional Periodic Information 25
Table 22: Error States 25

1 General

1.1 Overview

This non-proprietary FIPS 140-3 Security Policy for the Arista MACsec data plane accelerator [on-chip-driver], version 1.0 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 [on-chip-driver] consists of a hardware and the 3 software components that comprise the SDK MACsec FIPS Library, which is represented by the red dash line in Figure 5, below. The physical perimeter of the module is defined as the entire MACsec ASIC (BCM88850 and BCM88870). The software components of the module consists of the entire SDK MACsec FIPS Library.

The MACsec ASICs shown below, in Figures 1 and 3, represent the entire physical perimeter of the modules themselves and implement the core cryptographic functionality of the modules - AES-GCM/XPN encryption and decryption used within the MACsec protocol.

Tested Operational Environment's Physical Perimeter (TOEPP):

The Tested Operational Environment's Physical Perimeter consists of the **Arista DCS-7800R3AK-36DM2-LC (line card)** or **Arista DCS-7280R4K-32DE (standalone switch appliance)** that the modules reside within, which are represented in Figures 2 and 4, below. The tested operational environments are listed in Table Tested Operational Environments - Software, Firmware, Hybrid, below.

Figure 1: Broadcom BCM88850 physical perimeter.

Figure 2: Arista DCS-7800R3AK-36DM2-LC line card (TOEPP)

Figure 3: Broadcom BCM88870 physical perimeter.

Figure 4: Arista DCS-7280R4K-32DE switch (TOEPP)

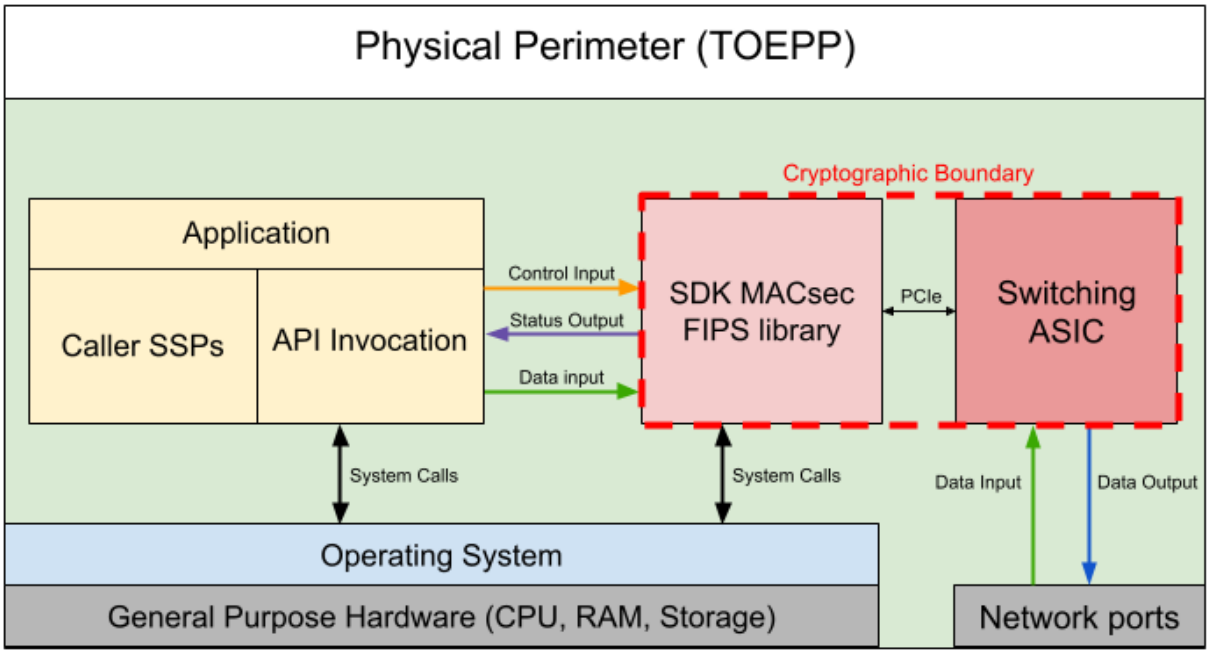

Figure 5: Module cryptographic boundary and TOEPP.

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
libfips_integrity_self_test.so	BCM/ Integrity self test version 2	Integrity self-test library which implements the SHA algorithm for all platforms	SHA2-256
libfips_sa_j2p.so	BCM/ J2P DNX FIPS SA 3	Secure association library implementing the APIs on the JC2+ platform	SHA2-256
libmini_access_cmicx_gen1.so	BCM/ Mini access CMICX gen1 version 2	Used for the PCIE driver to access the hardware and other components on the JC2+ platform	SHA2-256
libfips_sa_jr3.so	BCM/ JR3 DNX FIPS SA 3	Secure association library implementing the APIs on the Q3D platform	SHA2-256
libmini_access_cmicx_gen2.so	BCM/ Mini access CMICX gen2 version 1	Used for the PCIE driver to access the hardware and other components on the Q3D platform	SHA2-256

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
BCM88850	rev A0		BCM88850 rev A0	Single chip
BCM88870	rev A0		BCM88870 rev A0	Single chip

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
SONiC OS 12 (202511)	Arista DCS-7800R3AK-36DM2-LC	AMD EPYC 3201	No		BCM/ Integrity self test version 2 BCM/ J2P DNX FIPS SA 3 BCM/ Mini access CMICX gen1 version 2
SONiC OS 12 (202511)	Arista DCS-7280R4K-32DE	AMD Ryzen Embedded V3C48	No		BCM/ Integrity self test version 2 BCM/ JR3 DNX FIPS SA 3 BCM/ Mini access CMICX gen2 version 1

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

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

N/A for this module.

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:

Mode Name	Description	Type	Status Indicator
Approved mode	The approved mode of operation	Approved	POST_SUCCESS = 4

Table 5: 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:

Q3D (BCM88870)

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A5178	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A5178	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 128-1024 Increment 16 AAD Length - AAD Length: 128-1024 Increment 16	SP 800-38D
AES-XPN	A5178	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-1024 Increment 16 AAD Length - AAD Length: 128-1024 Increment 16 Tag Length - 128 IV Generation - External IV Generation Mode - Salt Generation - External	SP 800-38D

Table 6: Approved Algorithms - Q3D (BCM88870)

JC2+ (BCM88850)

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	C894	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	C894	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 1024, 8, 1016 AAD Length - AAD Length: 128, 1024, 8, 1016	SP 800-38D
AES-XPN	C894	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128, 1024, 8, 1016 AAD Length - AAD Length: 128, 1024, 8, 1016 Tag Length - 128 IV Generation - External Salt Generation - External	SP 800-38D

Table 7: Approved Algorithms - JC2+ (BCM88850)

Integrity Test Library

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A8001	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4

Table 8: Approved Algorithms - Integrity Test Library

The Approved Algorithms tables above list the approved algorithms implemented by Arista MACsec data plane accelerator [on-chip-driver].

Vendor-Affirmed Algorithms:

The module does not implement any vendor-affirmed algorithms.

Non-Approved, Allowed Algorithms:

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

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: (C894, A5178) AES-GCM: (C894, A5178) AES-XPN: (C894, A5178)
Decrypt Data	BC-Auth	Decryption of data in MACsec protocol	Publication:NIST SP 800-38D IG:C.H	AES-ECB: (C894, A5178) AES-GCM: (C894, A5178) AES-XPN: (C894, A5178)
Software Integrity Test	SHA	Integrity test for module software	Publication:FIPS 180-4	SHA2-256: (A8001)

Table 9: 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 and it's amendments.

While operating the approved mode of operation, the module should only be used to form a MACsec link with a separate FIPS 140 validated module operating in the approved mode. The device on each end of the MACsec link plays the role of either 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.

The link between the peer and authenticator module should be secured to prevent the possibility of an attack by introducing foreign equipment into the local area network.

2.8 RBG and Entropy

The module only generates SSPs used in the MACsec protocol deterministically. Therefore, the module does not implement 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 does not implement any key industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	Cryptographic keys via the API invocation on the Host CPU
PCIe interface receiver, Network Interface SERDES receiver, Fabric Interface SERDES receiver	Data Input	Plaintext data to be encrypted, Ciphertext data to be decrypted
PCIe interface transmitter, Network Interface SERDES transmitter, Fabric Interface SERDES transmitter	Data Output	Decrypted data (plaintext), Encrypted data (ciphertext)
N/A	Control Input	Control API function calls
N/A	Status Output	Return codes from API calls, Error/logging messages
1.5V Supply Pins	Power	Electrical power to the module's hardware component

Table 10: Ports and Interfaces

The Ports and Interfaces table above specifies the cryptographic module interfaces. The physical interfaces are defined as the PCIe interface transceiver, Network Interface Serializer/Deserializer transceiver and Fabric Interface Serializer/Deserializer transceiver of the MACsec chips. The logical interfaces are logically separated from one another by the software module design. The power interface is physically separate from the other physical interfaces as the pins that carry voltage are physically distinct from the pins which carry data to the PCIe and SERDES receivers.

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 11: 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 (show status) Check syslog (/var/log/syslog)	Status Output ("bcmXflowMacsecFipsStatePass (4)"	None	Crypto Officer
Show module's versioning info	Output the module name and version identifiers	Global (completion of service)	Command (show version)	Status Output ("BCM/ J2P DNX FIPS SA 3, BCM/ Mini access CMICX gen1 version 2, BCM/Integrity self test version 2" or "BCM/ JR3 DNX FIPS SA 3, BCM/ Mini access CMICX gen2 version 1, BCM/ Integrity self test version 2")	None	Crypto Officer
Perform self-tests on demand	Runs the software integrity check and cryptographic algorithm self	Global (completion of service)	Procedure/ Reboot	Status Output (pass/fail)	Software Integrity Test	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	tests on demand					
Zeroisation	Zeroise SSPs stored temporarily in RAM and in the chip registers	Global (completion of service)	Procedure/ Reboot	Status Output	None	Crypto Officer - AES-GCM Key: Z - AES-GCM IV: Z
Encrypt data	Encrypt plaintext data	Global (completion of service)	Function call/plaintext packets	Encrypted packets	Encrypt Data	Crypto Officer - AES-GCM Key: E - AES-GCM IV: G,E
Decrypt data	Decrypt ciphertext data	Global (completion of service)	Function call/encrypted packets	Plaintext packets	Decrypt Data	Crypto Officer - AES-GCM Key: E - AES-GCM IV: G,E
Security Association	Program encryption/decryption keys	Global (compl	Security Association Key (SAK)	Static return code indicating operation success	Encrypt Data	Crypto Offic

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
programming	for MACsec data plane traffic	etion of service)			Decrypt Data	er - AES-GCM Key: W
Security Association zeroization	Clear given Security Association	Global (completion of service)	Security Association identifier	Static return code indicating operation success	None	Crypto Officer - AES-GCM Key: Z

Table 12: Approved Services

The abbreviations of the access rights to SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

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

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 allow the loading of external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The approved integrity technique is implemented by the cryptographic module itself. The approved software integrity technique consists of a self-test, run pre-operationally.

Software integrity test:

The entire module software is covered with an approved integrity technique (SHA2-256) which is implemented in the module itself. If the calculated integrity value does not match the reference value installed with the software, the module enters the Error state and terminates execution of the module.

5.2 Initiate on Demand

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

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.

7 Physical Security

The 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 modifiable 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 chassis or appliance which is installed within a secure facility. The module will therefore inherit these additional physical characteristics and protections once deployed.

8 Non-Invasive Security

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

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 13: 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

Table 14: 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
Power Cycle/ Re-instantiate module	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
Security Association Zeroisation	Clear given Security Association (overwrite with 0's)	AES-GCM SAK is zeroised on command. Can also be zeroised by invoking the power-cycle method, above.	API call

Table 15: SSP Zeroization Methods

The Security Association Key (SAK) can be zeroised on demand by invoking the *Security Association Zeroisation* API service. Alternatively, all SSPs within the module can be zeroised by power-cycling/shutting down the module TOEPP.

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 - PSP	Encrypt Data Decrypt Data		Encrypt Data Decrypt Data

Table 16: 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	Power Cycle/ Re-instantiate module	AES-GCM IV:Used With
AES-GCM IV		Volatile Memory:Plaintext	Until zeroised	Power Cycle/ Re-instantiate module	AES-GCM Key:Used With

Table 17: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-256 (A8001)	SHA2-256 Approved hash compare	KAT	SW/FW Integrity	"INTEGRITY_PASS = 2" or "INTEGRITY_FAIL = 1"	Software component Integrity test using an approved hash

Table 18: Pre-Operational Self-Tests

The 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
AES-XPN (C894)	128 bits	KAT	CAST	"HW_KAT_FAIL = 3" or "POST_SUCCESS = 4"	Encrypt / Decrypt (using extended packet numbering function), MACsec ASIC	Before first operational use of encryption/decryption service. / Immediately when the module enters the approved mode of operation.
AES-XPN (A5178)	128 bits	KAT	CAST	"HW_KAT_FAIL = 3" or "POST_SUCCESS = 4"	Encrypt / Decrypt (using extended packet numbering function), MACsec ASIC	Before first operational use of encryption/decryption service. / Immediately when the module enters the approved mode of operation.
SHA2-256 (A8001)	SHA2-256 Approved hash compare	KAT	CAST	"HW_KAT_FAIL = 3" or "POST_SUCCESS = 4"	Hash compare - CAST for integrity function	Before first operational use of the approved integrity mechanism/ Immediately when

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						the module enters the approved mode of operation.

Table 19: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A8001)	KAT	SW/FW Integrity	On Demand / On Startup	Manually, by reboot of host device

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XPN (C894)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
AES-XPN (A5178)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device
SHA2-256 (A8001)	KAT	CAST	On Demand / On Startup	Manually, by reboot of host device

Table 21: Conditional Periodic Information

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

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	Module terminates operation, Host device must be restarted	Module fails SHA2-256 CAST, Software Integrity Test, or AES-XPN CAST	Reboot host platform	"INTEGRITY_FAIL = 1" or "HW_KAT_FAIL = 3"

Table 22: Error States

When the module fails any self-test, the module will immediately print a self-test failure indicator to the device log. When in the error state, the TOEPP's interfaces will not be available and therefore, all cryptographic operation is inhibited.

10.5 Operator Initiation of Self-Tests

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

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Arista MACsec data plane accelerator [on-chip-driver] is pre-installed and configured by Arista before delivering the platform to their clients. 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.

11.4 Additional Information

Building the *Arista MACsec data plane accelerator [on-chip-driver]* from source:

The Arista MACsec data plane accelerator [on-chip-driver] module is distributed as part of the Broadcom Software Development Kit (SDK) 6.5.34 SP3. To build the SDK with cryptographic module support, the SDK should be compiled with the XFLOW_MACSEC_FIPS compilation flag.

Alternatively, the cryptographic module can be built standalone using the following steps:

```
cd sdk-macsec-6.5.34-SP3/src/bcm/dnx/fips
make all
cp *.so *.sha256 {INSTALL_PATH}
```

To verify that the cryptographic module is properly installed and operating in approved mode of operation the following command sequence should be executed:

```
bcmsh
cint
int unit = 0;
int flags = 0;
bcm_xflow_macsec_fips_version_t version_info;
bcm_xflow_macsec_fips_version_get(unit, flags, &version_info);
printf("Show version service output: %s\n", version_info.version);
bcm_xflow_macsec_instance_id_t instance = 0;
bcm_xflow_macsec_fips_state_t state;
bcm_xflow_macsec_fips_state_get( unit, flags, instance, &state );
print state;
```

When the above show status service outputs the following string:

bcm_xflow_macsec_fips_state_t state = bcmXflowMacsecFipsStatePass (4)
It means that the module is properly operating in approved mode of operation.

12 Mitigation of Other Attacks

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