Arista Networks, Inc.

Arista MACsec data plane accelerator [on-chip]

Version: 1.0

FIPS 140-3 Non-Proprietary Security Policy

Document prepared by:

http://www.lightshipsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This non-proprietary FIPS 140-3 Security Policy for the Arista MACsec Module, 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	N/A
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 and IPsec 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: Hardware

Module Embodiment: Single Chip

Cryptographic Boundary:

The cryptographic boundary of the Arista MACsec Module consists of a hardware and a firmware component executing within that hardware, which is represented by the red dash line in Figure 10, below. The physical perimeter of the module is defined as the entire Broadcom ASIC. The sole firmware component of the module consists of the .srec file for the particular chip, which is contained in MacsecFips.rpm.

Tested Operational Environment's Physical Perimeter (TOEPP):

The single chips shown below represent the entire physical perimeter and implement the core cryptographic functionality of the module, AES-GCM encryption and decryption used within the MACsec and IPsec protocols.

Figure 1: Broadcom BCM88850 physical perimeter.

Figure 2: Broadcom BCM88852 physical perimeter.

Figure 3: Broadcom BCM88859 physical perimeter.

Figure 4: Broadcom BCM56070 physical perimeter.

Figure 5: Broadcom BCM56071 physical perimeter.

Figure 6: Broadcom BCM56782 physical perimeter.

Figure 7: Broadcom BCM88860 physical perimeter.

Figure 8: Broadcom BCM88490 physical perimeter.

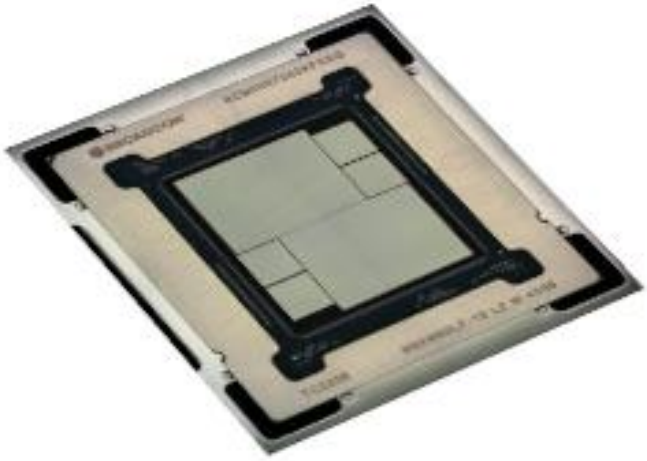

Figure 9: Broadcom BCM88870 physical perimeter.

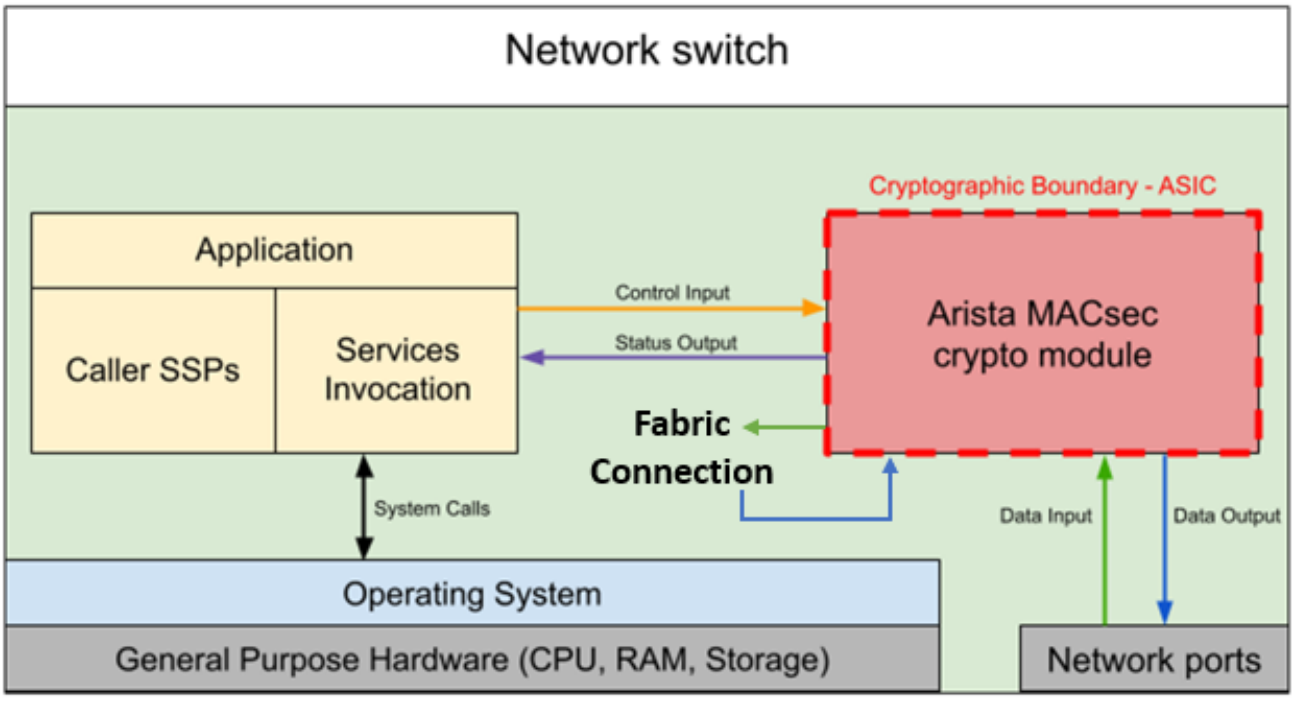

Figure 10: Module cryptographic boundary and TOEPP.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Broadcom BCM88850	Rev A2	fips-jericho2cplus.srec, v1.0	BCM88850	Broadcom Jericho2c+
Broadcom BCM88852 (rev. A1)	Rev A1	fips-jericho2cplus.srec, v1.0	BCM88852	Broadcom Jericho2c+
Broadcom BCM88852 (rev. A2)	Rev A2	fips-jericho2cplus.srec, v1.0	BCM88852	Broadcom Jericho2c+
Broadcom BCM88859	Rev A2	fips-jericho2cplus.srec, v1.0	BCM88859	Broadcom Jericho2c+
Broadcom BCM56070	Rev A0	fips-firelight.srec, v1.0	BCM56070	Broadcom Firelight
Broadcom BCM56071	Rev A0	fips-firelight.srec, v1.0	BCM56071	Broadcom Firelight
Broadcom BCM56782	Rev A1	fips-t4x9.srec, v1.0	BCM56782	Broadcom Trident4
Broadcom BCM88860	Rev B0	fips-jericho3.srec, v1.0	BCM88860	Broadcom Jericho3
Broadcom BCM88490	Rev B0	fips-qumran3a, v1.0	BCM88490	Broadcom Qumran3A
Broadcom BCM88870	Rev A0	fips-jericho3.srec, v1.0	BCM88870	Broadcom Qumran3D

Table 2: Tested Module Identification – Hardware

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	device log (SUCCESS)

Table 3: 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:

Other chips

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A5178	Direction - Encrypt Key Length - 128, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A5178	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - Key Length - 128, 256	SP 800-38D
AES-GMAC	A5178	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D
AES-XPN	A5178	Direction - Decrypt, Encrypt Key Length - 128, 256 IV Generation - External IV Generation Mode -	SP 800-38D

Table 4: Approved Algorithms - Other chips

Firelight-based chips

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	SP 800-38D
AES-GMAC	A5336	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D
AES-XPN	C894	Direction - Decrypt, Encrypt Key Length - 128, 256 IV Generation - External	SP 800-38D

Table 5: Approved Algorithms - Firelight-based chips

The Approved Algorithms tables above list the approved algorithms implemented by the Arista MACsec Module.

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 using AES-GCM/XPN	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 using AES-GCM/XPN	Publication:NIST SP 800-38D IG:C.H	AES-ECB: (C894, A5178) AES-GCM: (C894, A5178) AES-XPN: (C894, A5178)
Firmware Integrity Test	MAC	Integrity check using the built-in AES-GCM functionality of the chip (AES-GMAC)		AES-GMAC: (A5336, A5178)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

Within MACsec protocol:

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.

Within IPsec protocol:

The AES-CGM Initialization Vector (IV) generation is compliant with IG C.H, resolution 1(b). The module generates IVs in compliance with RFC5282.

In case the module's power is lost, or the IKE/IPsec connection is terminated, the SA must be renegotiated to restore connectivity.

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 in accordance with the following guidance:

MACsec – The IV is constructed following the guidance given in IG C.H, resolution 1(c) and IEEE802.1AE.

IPsec – The IV is constructed following the guidance given in IG C.H, resolution 1(b) and RFC5282 and RFC4106.

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.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCIE_RX, NIF50_RX, FAB50_RX	Data Input	Plaintext data to be encrypted, Encrypted data to be decrypted
PCIE_TX, NIF50_TX, FAB50_TX	Data Output	Plaintext data that has been decrypted, Encrypted data that has been encrypted
PCIE_RX	Control Input	Command signal invoking cryptographic services
PCIE_TX	Status Output	Status information regarding the module and the invoked service/function.
PCIE_VDDHRX1P5, PCIE_VDDHTX1P5: Voltage=1.5V	Power	Electrical power to the module

Table 7: 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 Broadcom chips. The logical interfaces are logically separated from one another by the firmware 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.

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 8: 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 (SUCCESS, POST_FAIL)	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 [on-chip] v1.0")	None	Crypto Officer
Perform Self-tests	Runs the firmware integrity check and cryptographic algorithm self tests on demand	Global (completion of service)	Command/Procedure	Status Output	Firmware Integrity Test	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform Zeroisation	Zeroise SSPs stored temporarily in RAM	Global (completion of service)	Command/Procedure	Status Output	None	Crypto Officer - AES-GCM Key: Z - AES-GCM IV (MACsec): Z - AES-GCM IV (IPsec): 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 (MACsec): G,E - AES-GCM IV (IPsec): 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 (MACsec): G,E - AES-GCM IV (IPsec): G,E
Establish Encrypted Session	Output initial packet with no payload to the MACsec implementati	Global (completion of service)	Traffic + Parameters	Plaintext Data (Initial Packet Header)	Encrypt Data Decrypt Data	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	on to establish MACsec session using packet header					

Table 9: Approved Services

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 loads the appropriate .srec file for the ASIC present in the device from MacsecFips.rpm upon each reboot in compliance with FIPS IG 10.3.F, additional comment 3.

Any firmware image that is not shown on the module certificate is out of scope of this validation and requires a separate FIPS 140-3 validation.

5 Software/Firmware Security

5.1 Integrity Techniques

The module's firmware integrity self-test is managed within the module boundary by the module firmware itself. The module passes the entire module .srec file to the GCM implementation of the ASIC as the Authenticated Payload. The module then compares the output ICV with the expected ICV value, which is embedded in the .rpm file and independently loaded. If the expected values do not match, the integrity test fails, and the module enters the error state.

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).

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-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

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 module firmware executes entirely within programmable ASIC chip, the module is defined as a hardware module with a single-chip 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.

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 10: 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	External	Volatile Memory	Plaintext	Automated	Electronic	Decrypt Data

Table 11: 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 security level 1.	Crypto Officer reboots or removed power from host platform

Table 12: SSP Zeroization Methods

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

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		Encrypt Data Decrypt Data
AES-GCM IV (MACsec)	Initialization Vector for AES-GCM MACsec encryption	96 bits - N/A	Initialization Vector - PSP	Encrypt Data Decrypt Data		Encrypt Data Decrypt Data
AES-GCM IV (IPsec)	Initialization Vector for AES-GCM IPsec encryption	64 bits - N/A	Initialization Vector - PSP	Encrypt Data Decrypt Data		Encrypt Data Decrypt Data

Table 13: SSP Table 1

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

Table 14: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
AES-GMAC (A5336)	AES-GMAC	KAT	SW/FW Integrity	log ("INTEGRITY_CHECK_SUCCESS" = pass, "INTEGRITY_CHECK_FAIL" = fail)	Calculate MAC of entire module firmware and compare to known answer

Table 15: 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
AES-XPN (C894)	256 bits	KAT	CAST	log ("SUCCESS" = pass "POST_FAIL" - fail)	Encrypt / Decrypt (using extended packet numbering function), covers firelight-based chips	Before first operational use of AES-GCM/AES-GMAC. Immediately when the module enters the approved mode of operation.
AES-XPN (A5178)	256 bits	KAT	CAST	log ("SUCCESS" = pass "POST_FAIL" - fail)	Encrypt / Decrypt (using extended packet numbering function), Covers non-firelight chips	Before first operational use of AES-GCM/AES-GMAC. Immediately when the module enters the approved mode of operation.

Table 16: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GMAC (A5336)	KAT	SW/FW Integrity	Upon module startup	Manual (reboot host platform)

Table 17: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XPN (C894)	KAT	CAST	On Demand / On Startup	Manually
AES-XPN (A5178)	KAT	CAST	On Demand / On Startup	Manually

Table 18: 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
Error	Hard Error State: MACsec interfaces do not come up, traffic blocked	Module fails any self-test	Reboot host platform	log ("POST_FAIL" or "INTEGRITY_CHECK_FAIL")

Table 19: Error States

When the module fails any self-test, the module will immediately print a self-test failure indicator to the device log (*"POST_FAIL"*). 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 Module 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 for the approved mode indicator which consists of the chip name, module name and version, and pass/fail result of the module integrity test.

See the following example output for the module using the BCM88852 chip:

Detected Jericho2cPlus (0x8852)
module_name_ver "Arista MACsec data plane accelerator [on-chip] v1.0"
init_status SUCCESS(9)

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

The *Arista MACsec data plane accelerator [on-chip]* cryptographic module is available in the following Arista platforms:

Operating System: Arista EOSv4

Hardware Platform:

- Arista DCS-7280DR3AK-36S
- Arista 7800R3A
- Arista DCS-7280DR3AM-54
- Arista 7280CR3AM-32S
- Arista CCS-750-SUP100
- Arista CCS-750X-48TP-LC
- Arista DCS-7050CX4M-48D8
- Arista 7800R4K-36PE-LC
- Arista DCS-7020R4M-48Y-8QC
- Arista DCS-7280R4K-32PE
- Arista 7289R3AK-SC
- Arista 7289R3AM-SC
- Arista DCS-7800R3A-36DM-LC
- Arista DCS-7800R3A-36PM-LC
- Arista DCS-7800R3AK-36DM-LC
- Arista DCS-7800R3AK-36DM2-LC
- Arista DCS-7800R3AK-36PM-LC
- Arista DCS-7800R3A-36DM2-LC
- Arista DCS-7800R4M-36PE-LC
- Arista CCS-750-SUP25
- Arista CCS-750X-48SX-LC
- Arista CCS-750X-48THP-LC

- Arista CCS-750X-48ZP-LC
- Arista CCS-750X-48ZXP-LC
- Arista DCS-7280CR3AK-32S
- Arista DCS-7280DR3AK-36
- Arista DCS-7280DR3AK-54
- Arista DCS-7280DR3AM-36
- Arista DCS-7280SR3AK-48YC8
- Arista DCS-7280SR3AM-48YC8
- Arista DCS-7280R4K-32DE

The vendor affirms that the cryptographic module operates identically in other environments not listed above.

12 Mitigation of Other Attacks

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