Arista Networks, Inc.

Arista Crypto Module

FIPS 140-3 Non-Proprietary Security Policy

August 8th, 2024

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 Cryptographic Module, v4.0 describes how the module meets the security requirements specified in FIPS 140-3 (Federal Information Processing Standard 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	N/A
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	1
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module is a dynamic software library providing an application programming interface (API) intended to be used via OpenSSL interfaces to serve cryptographic functionalities for applications running in the user space of the underlying operating system.

Module Type: Software

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The module's cryptographic boundary (represented by the red dotted line in Figure 1) consists of the entire Arista Cryptographic Module executable code.

Tested Operational Environment's Physical Perimeter (TOEPP):

The module was tested on the Arista AWE-5510 router, running Arista's EOS operating system.

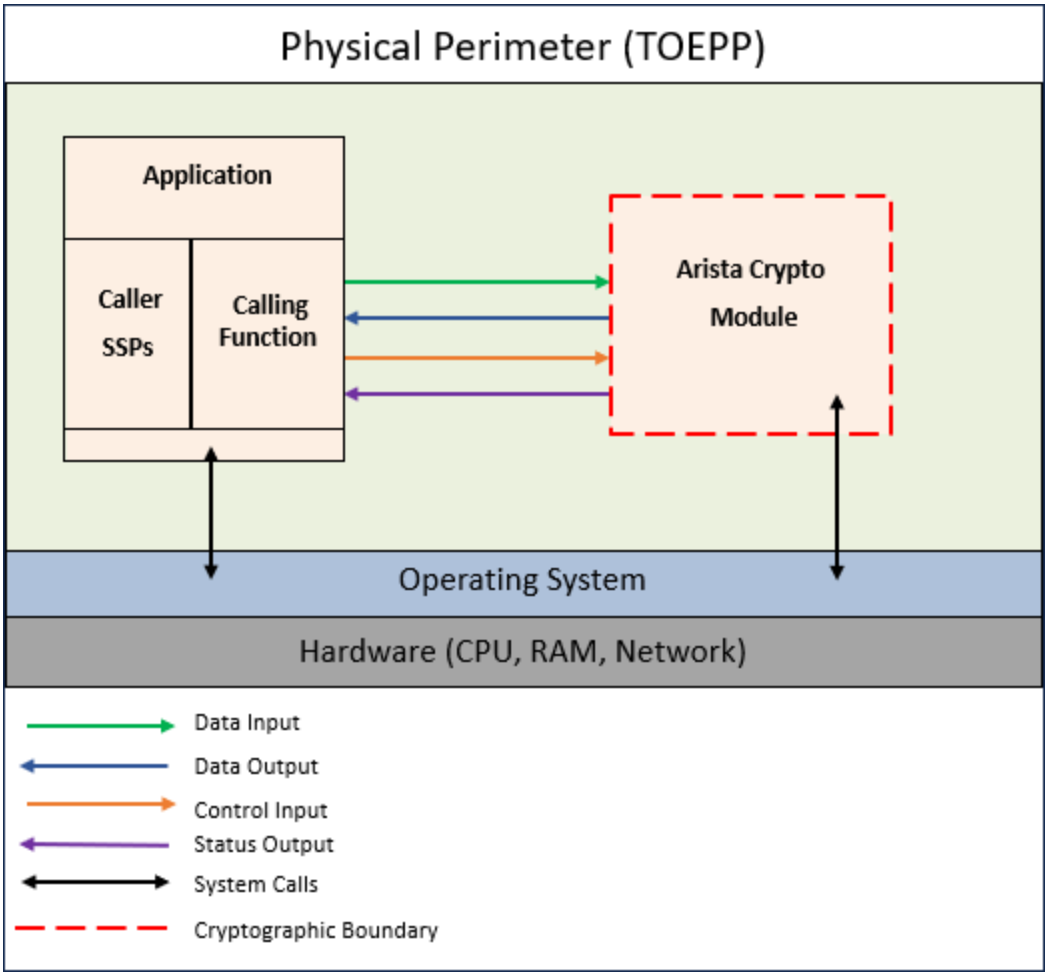

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
fips.so	v4.0	RPM package containing module in executable format	HMAC-SHA2-256

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
EOSv4	Arista AWE-5510	Intel® Xeon® Processor D-2798NX (Ice Lake)	Yes		v4.0
EOSv4	Arista AWE-5510	Intel® Xeon® Processor D-2798NX (Ice Lake)	No		v4.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

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

Operating System	Hardware Platform
EOSv4	Arista 7289 with Intel Xeon CPU D-1548
EOSv4	Arista 7300-SUP-D with Intel Xeon CPU @ 2.60GHz
EOSv4	Arista 7368-SUP with Intel Xeon CPU D-1527
EOSv4	Arista 7368-SUP-D with Intel Xeon CPU D-1527
EOSv4	Arista 7388-SUP-D with Intel Xeon CPU D-1527
Linux 5.4	Arista C-460 with ARM Cortex-A73
Linux 5.4	Arista O-435 with ARM Cortex-A53
EOSv4	Arista AWE-5310 with Intel Atom P5721
EOSv4	Arista AWE-5310-2F-FLX with Intel Atom P5721
EOSv4	Arista AWE-5510 with Intel Xeon D-2798NX CPU
EOSv4	Arista AWE-5510-2F-FLX with Intel Xeon D-2798NX
EOSv4	Arista AWE-7220RP-5TH-2S with Intel Atom CPU C3558R
EOSv4	Arista AWE-7230R-4TX-4S-FLX with Intel Atom P5721
EOSv4	Arista AWE-7250R-16S-FLX with Intel Xeon D-2798NX
EOSv4	Arista CCS-710P-12 with AMD GX-412TC
EOSv4	Arista CCS-710P-12-NA with AMD GX-412TC
EOSv4	Arista CCS-710P-16P with AMD GX-412TC
EOSv4	Arista CCS-710P-16P-NA with AMD GX-412TC
EOSv4	Arista CCS-720DF-48Y with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DF-48Y-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DF-48Y-DC with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DF-48Y-M-S-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DP-24S with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DP-24S-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DP-24S-M-S-2 with AMD Ryzen Embedded R1600

Operating System	Hardware Platform
EOSv4	Arista CCS-720DP-24ZS-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DP-48S with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DP-48S-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DP-48S-M-S-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DP-48ZS with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DT-24S with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DT-24S-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DT-24S-2R with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DT-24S-M-S-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DT-48S with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720DT-48S-2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720XP-24Y6 with AMD Crowned Eagle GX-224PC or AMD G-Series GX-224
EOSv4	Arista CCS-720XP-24ZY4 with AMD Crowned Eagle GX-224PC or AMD G-Series GX-224
EOSv4	Arista CCS-720XP-48TXH-2C-S with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720XP-48Y6 with AMD Crowned Eagle GX-224PC or AMD G-Series GX-224
EOSv4	Arista CCS-720XP-48ZC2 with AMD Crowned Eagle GX-224PC or AMD G-Series GX-224
EOSv4	Arista CCS-720XP-48ZXC2 with AMD Ryzen Embedded R1600
EOSv4	Arista CCS-720XP-96ZC2 with AMD R-Series RX-216 (Merlin Falcon)
EOSv4	Arista CCS-720XP-96ZC2-M-S-4 with AMD Embedded R-Series RX-216TD
EOSv4	Arista CCS-720XP-96ZC2-M-S with AMD Embedded R-Series RX-216TD
EOSv4	Arista CCS-722XPM-48Y4 with AMD G-Series GX-224 (Crowned Eagle)
EOSv4	Arista CCS-722XPM-48ZY8 with AMD G-Series GX-224 (Crowned Eagle)
EOSv4	Arista CCS-750-SUP100 with Intel Xeon D-1527 (Broadwell)
EOSv4	Arista CCS-750-SUP25 with Intel Xeon D-1527 (Broadwell)
CloudVision Portal	Any general-purpose computer (GPC) with Any CPU
CloudVision Portal on VMware ESXi 6.7 on AlmaLinux 9	Supermicro SYS-6029TP-HTR with Intel Xeon Gold 5218R

Operating System	Hardware Platform
CloudVision Portal on QEMU 2.12 on AlmaLinux 9	Supermicro SYS-6029TP-HTR with Intel Xeon Silver 4316
CloudEOSv4	Any general-purpose computer (GPC) with Any CPU
CloudEOSv4 on QEMU 2.0	Supermicro SYS-1029U-TR-CTO with Intel Xeon Gold 6240R
EOSv4	Arista DCS-7010T-48 with AMD eKabini GX-210HA or AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7010T-48-DC with AMD eKabini GX-210HA or AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7010TX-48 with AMD Crowned Eagle GE224PIXJ23JB
EOSv4	Arista DCS-7010TX-48-DC with AMD Crowned Eagle GE224PIXJ23JB
EOSv4	Arista DCS-7010TX-48C with AMD Ryzen Embedded R1600
EOSv4	Arista DCS-7010TX-48C-DC-RV3 with AMD Ryzen Embedded R1600
EOSv4	Arista DCS-7020SR-24C2 with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7020SR-32C2 with Intel Broadwell DE D1508
EOSv4	Arista DCS-7020SRG-24C2 with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7020TR-48 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7020TRA-48 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7050CX3-32C with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050CX3-32S with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7050CX3-32S-SSD with AMD GX-424CC SOC
EOSv4	Arista DCS-7050CX3M-32S with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7050CX4-24D8 with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050CX4-40D with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050CX4-48D8 with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050CX4M-48D8 with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050DX4-32S with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7050DX4M-32S with AMD Snowy Owl SP4r2 3151
EOSv4	Arista DCS-7050PX4-32S with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)

Operating System	Hardware Platform
EOSv4	Arista DCS-7050QX-32 with AMD Athlon NEO X2 N40L
EOSv4	Arista DCS-7050QX-32S with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050QX2-32S with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7050SDX4-48D8 with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050SPX4-48D8 with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050SX-128 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7050SX-64 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050SX-72 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050SX-72Q with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7050SX-96 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050SX2-128 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7050SX2-72Q with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7050SX3-48C8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7050SX3-48C8C with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050SX3-48YC12 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7050SX3-48YC8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7050SX3-48YC8C with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7050SX3-96YC8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7050TX-128 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7050TX-48 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050TX-64 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050TX-72 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050TX-72Q with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7050TX-96 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7050TX2-128 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)

Operating System	Hardware Platform
EOSv4	Arista DCS-7050TX3-48C8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7060CX-32C with AMD GX-424PC SOC
EOSv4	Arista DCS-7060CX-32S with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7060CX2-32S with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7060CX5-56D8 with AMD Ryzen Embedded V1500B
EOSv4	Arista DCS-7060DX4-32 with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7060DX5-32 with AMD EPYC 3151 (4c or 8c)
EOSv4	Arista DCS-7060DX5-64 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7060DX5-64E with AMD EPYC Embedded 3151
EOSv4	Arista DCS-7060DX5-64S with AMD EPYC Embedded 3151
EOSv4	Arista DCS-7060PX4-32 with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7060PX5-64 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7060PX5-64E with AMD EPYC Embedded 3151
EOSv4	Arista DCS-7060PX5-64S with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7060SX2-48YC6 for AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7060X6-64PE with AMD EPYC 3151 (4c or 8c)
EOSv4	Arista DCS-7130-16G3S with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-48EHS with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-48G3S with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-48LAS with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-48LBAS with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-48LBS with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-96LAS with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-96LBAS with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-96LBS with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130-96LS with Intel Atom® Processor C2558 (Rangeley)

Operating System	Hardware Platform
EOSv4	Arista DCS-7130-96S with Intel Atom® Processor C2558 (Rangeley)
EOSv4	Arista DCS-7130LBR-48S6QD with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7132LB-48Y4C with AMD EPYC 3251
EOSv4	Arista DCS-7132LB-48Y4C-DC with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7132LN-48Y4C with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7135LB-48Y4C with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7148SX with AMD Athlon NEO X2 N40L
EOSv4	Arista DCS-7150S-24-CL with AMD Athlon NEO X2 N40L
EOSv4	Arista DCS-7150SC-24-CLD with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7150SC-64-CLD with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7160-32CQ with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7160-48TC6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7160-48YC6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7170-32C with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7170-32CD with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7170-64C with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7170B-64C with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7260CX-64 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7260CX3-64 with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7260CX3-64E with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7260CX3-64LQ with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7260QX-64 with Intel "Gladden" Sandy Bridge or AMD GX-424CC SOC
EOSv4	Arista DCS-7280CR-48 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7280CR2-60 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7280CR2A-30 with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7280CR2A-60 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7280CR2K-30 with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7280CR2K-60 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7280CR2M-30 with Intel Broadwell-DE D1508
EOSv4	Arista DCS-7280CR3-32D4 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD

Operating System	Hardware Platform
EOSv4	Arista DCS-7280CR3-32P4 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3-36S with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3-96 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3A-24D12 with AMD Snowy Owl SP4r2 3251
EOSv4	Arista DCS-7280CR3A-32S with AMD EPYC 3251
EOSv4	Arista DCS-7280CR3A-48D6 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280CR3A-72 with AMD Snowy Owl SP4r2 3251
EOSv4	Arista DCS-7280CR3AK-24D12 with AMD Snowy Owl SP4r2 3251
EOSv4	Arista DCS-7280CR3AK-48D6 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280CR3AK-72 with AMD Snowy Owl SP4r2 3251
EOSv4	Arista DCS-7280CR3AM-24D12 with AMD Snowy Owl SP4r2 3251
EOSv4	Arista DCS-7280CR3AM-32S with AMD EPYC 3251
EOSv4	Arista DCS-7280CR3AM-48D6 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280CR3AM-72 with AMD Snowy Owl SP4r2 3251
EOSv4	Arista DCS-7280CR3E-36S with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3K-32D4 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3K-32D4A with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280CR3K-32P4 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3K-32P4A with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280CR3K-36A with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280CR3K-36S with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3K-96 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD

Operating System	Hardware Platform
EOSv4	Arista DCS-7280CR3MK-32D4 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3MK-32D4A-S with AMD EPYC 3251
EOSv4	Arista DCS-7280CR3MK-32D4S with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3MK-32P4 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280CR3MK-32P4S with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280DR3-24 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280DR3A-36 with AMD EPYC Embedded 3251
EOSv4	Arista DCS-7280DR3A-54 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280DR3AK-36 with AMD EPYC Embedded 3251
EOSv4	Arista DCS-7280DR3AK-36S with AMD EPYC 3251
EOSv4	Arista DCS-7280DR3AK-54 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280DR3AM-36 with AMD EPYC Embedded 3251
EOSv4	Arista DCS-7280DR3AM-54 with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280DR3K-24 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280PR3-24 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280PR3K-24 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280QR-C36 with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7280QR-C72 with Intel "Gladden" Sandy Bridge
EOSv4	Arista DCS-7280QRA-C36S with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7280SE-64 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7280SE-68 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7280SE-72 with AMD eKabini GE420CIAJ44HM
EOSv4	Arista DCS-7280SR-48C6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)

Operating System	Hardware Platform
EOSv4	Arista DCS-7280SR2-48YC6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7280SR2A-48YC6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7280SR2K-48C6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7280SR3-40YC6 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280SR3-48YC8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280SR3A-48YC8 with AMD EPYC 3251
EOSv4	Arista DCS-7280SR3AM-48YC8 with AMD EPYC 3251
EOSv4	Arista DCS-7280SR3E-40YC6 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280SR3E-40YC6-M with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280SR3E-48YC8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280SR3K-48YC8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280SR3K-48YC8A with AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
EOSv4	Arista DCS-7280SR3M-48YC8 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280SR3MK-48YC8A-S with AMD EPYC 3251
EOSv4	Arista DCS-7280SRA-48C6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7280SRAM-48C6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7280SRM-40CX2 with AMD Steppe Eagle GE424CIXJ44JB
EOSv4	Arista DCS-7280TR-48C6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7280TR3-40C6 with AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
EOSv4	Arista DCS-7280TRA-48C6 with AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
EOSv4	Arista DCS-7289-SUP with Intel Xeon CPU D-1548
EOSv4	Arista DCS-7289-SUP-S with Intel Xeon CPU D-1548
EOSv4	Arista DCS-7300-SUP with Intel Xeon CPU @ 2.60GHz

Operating System	Hardware Platform
EOSv4	Arista DCS-7300-SUP2-D with Intel Xeon CPU D-1528
EOSv4	Arista DCS-7388-SUP with Intel Sandy Bridge Gladden AV8062701048500 or Intel Xeon CPU D-1527
EOSv4	Arista DCS-7500-SUP2 with Intel Xeon CPU D-1528
EOSv4	Arista DCS-7500-SUP2-D with Intel Xeon CPU D-1531
EOSv4	Arista DCS-7516-SUP2 with Intel Xeon CPU D-1548
EOSv4	Arista DCS-7800-SUP with Intel Xeon CPU D-1528
EOSv4	Arista DCS-7800-SUP1A with Intel Broadwell DE D-1528
EOSv4	Arista DCS-7800-SUP1S with Intel Broadwell DE D-1528
EOSv4	Arista DCS-7800A-SUP1A with Intel Xeon CPU D-1528
EOSv4	Arista DCS-7816-SUP with Intel Broadwell DE D-1548
EOSv4	Arista DCS-7816-SUP1S with Intel Broadwell DE D-1548
EOSv4	Arista ZTX-7250F-16S with Intel Xeon D-2798NX
EOSv4	Arista ZTX-7250S-16S with Intel Xeon D-2798NX
EOSv4	Arista DCS-7060X6-64DE
EOSv4	Arista 7280CR3AK-32S
EOSv4	Arista 7280SR3AK-48YC8
Linux 4.4	Arista C-200
Linux 4.4	Arista C-230
Linux 4.4	Arista C-230E
Linux 4.4	Arista C-260
Linux 4.4	Arista C-330
Linux 4.4	Arista C-360
Linux 5.4	Arista C-460E
Linux 4.4	Arista O-235
Linux 4.4	Arista O-235E
Linux 4.4	Arista W318
Linux 4.4	Arista W318-RW
CloudVision-CUE on CloudVision Portal on any hypervisor	Any general-purpose computer (GPC) with any CPU

Table 4: 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 components excluded from the module's cryptographic boundary or the FIPS security requirements.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	State in which the module is performing approved cryptographic services	Approved	1 (return code)
Non-Approved Mode	State in which the module is performing non-approved cryptographic services (TDES)	Non-Approved	0 (return code)

Table 5: Modes List and Description

The module is able to alternate between the approved and non-approved mode of operation based on service invocation.

In the non-approved mode of operation, the module can offer Triple-DES encryption and decryption. When the Triple-DES encrypt and decrypt services are called, the module transitions to the non-approved state and a static return code of '0', representing the invocation of a non-approved service is returned from the module.

2.5 Algorithms

Approved Algorithms:

The table below lists the approved cryptographic algorithms of the module and implemented modes of operation of the algorithms.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A5259	Key Length - 128, 192, 256	SP 800-38C
AES-CFB1	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A5259	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A5259	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F

Algorithm	CAVP Cert	Properties	Reference
AES-KWP	A5259	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-XTS Testing Revision 2.0	A5259	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A5259	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5259	Curve - P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A5259	Curve - P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5259	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A5259	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A5259	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
Hash DRBG	A5259	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512, SHA3-256, SHA3-512	SP 800-90A Rev. 1
HMAC DRBG	A5259	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512, SHA3-256, SHA3-512	SP 800-90A Rev. 1
HMAC-SHA-1	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-384	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5259	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5259	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A5259	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv1 (CVL)	A5259	Authentication Method - Pre-shared Key Preshared Key Length - Preshared Key Length: 8-8192 Increment 8 Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 1024-8192 Increment 1024 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF IKEv2 (CVL)	A5259	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 1024-8192 Increment 1024 Derived Keying Material Length - Derived Keying Material Length: 256-2048 Increment 128 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SP800-108	A5259	KDF Mode - Counter Supported Lengths - Supported Lengths: 128, Supported Lengths: 8-1536 Increment 8	SP 800-108 Rev. 1
KDF SSH (CVL)	A5259	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KTS-IFC	A5259	Modulo - 2048, 3072, 4096 Key Generation Methods - rsakpg2-basic Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Key Length - 512	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A5259	Key Generation Mode - probable, probableWithProbableAux Modulo - 2048, 3072, 4096	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
		Primality Tests - 2powSecStr Private Key Format - standard	
RSA SigGen (FIPS186-5)	A5259	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A5259	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A5259	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-224	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-256	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-384	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA2-512	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 180-4
SHA3-224	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 202
SHA3-256	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 202
SHA3-384	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 202
SHA3-512	A5259	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 4	FIPS 202
TLS v1.2 KDF RFC7627 (CVL)	A5259	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

The vendor affirms the approved implementation of the following security methods:

Name	Properties	Implementation	Reference
CKG (Asymmetric)	Key Type:Asymmetric	Arista Crypto Module	NIST SP 800-133rev2, Section 4 (1), 5.1, 5.2

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

The module does not implement any non-approved algorithms allowed in the approved mode of operation.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

The module does not implement any non-approved algorithms, allowed in the approved mode of operation, with no security claimed.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
Triple-DES	Encryption/decryption

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Data Encryption	BC-Auth BC-UnAuth	Symmetric Encryption	key size:128, 192, 256 bits	AES-CBC AES-CCM AES-CFB1 AES-CFB128 AES-CFB8 AES-CTR AES-ECB AES-GCM AES-XTS Testing Revision 2.0
Data Decryption	BC-Auth BC-UnAuth	Symmetric Encryption	key size:128, 192, 256	AES-CBC AES-CCM AES-CFB1 AES-CFB128 AES-CFB8 AES-CTR AES-ECB AES-GCM AES-XTS

Name	Type	Description	Properties	Algorithms
				Testing Revision 2.0
Key Derivation Function	KAS-135KDF KBKDF	Key Derivation Function		KDF IKEv1 KDF IKEv2 KDF SSH TLS v1.2 KDF RFC7627 KDF SP800-108
Deterministic Random Bit Generation	DRBG	Deterministic Random Bit Generation		Counter DRBG Hash DRBG HMAC DRBG
Digital Signature	DigSig-SigGen DigSig-SigVer	RSA, ECDSA SigGen / SigVer		ECDSA SigGen (FIPS186-5) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-5)
Message Authentication	MAC	Generate or verify data integrity		AES-CMAC HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512
Key Agreement ECC	KAS-SSC	Perform key agreement primitives on behalf of the calling process (does not establish keys into the module)	Security Strength:Key establishment methodology provides between 112 and 256 bits of encryption	KAS-ECC-SSC Sp800-56Ar3

Name	Type	Description	Properties	Algorithms
			strength. Publication:NIST SP 800-56Arev3 IG:D.F - Scenario 2, Path (1)	
Key Agreement FFC	KAS-SSC	Perform key agreement primitives on behalf of the calling process (does not establish keys into the module)	Security Strength:Key establishment methodology provides between 112 and 200 bits of encryption strength. Publication:NIST SP 800-56Arev3 IG:D.F - Scenario 2, Path (1)	KAS-FFC-SSC Sp800-56Ar3
Message digest	SHA	Hashing		SHA-1 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Key Generation	AsymKeyPair-KeyGen	Key Generation (asymmetric)	Publication:NIST SP 800-133rev2 - Section 4 Publication:NIST SP 800-133rev2 - Section 5 Publication:NIST SP 800-133rev2 - Section 6.2.2	ECDSA KeyGen (FIPS186-5) ECDSA KeyVer (FIPS186-5) KAS-ECC-SSC Sp800-56Ar3 KAS-FFC-SSC Sp800-56Ar3 RSA KeyGen (FIPS186-5) CKG (Asymmetric) Key Type: Asymmetric CKG Key Type: KBKDF Derived Key
Key Transport	KTS-Encap	Key Transport (encapsulation)	Security Strength:Key	KTS-IFC

Name	Type	Description	Properties	Algorithms
		using RSA-OAEP	establishment methodology provides between 112 and 150 bits of encryption strength.	
Key Wrapping	KTS-Wrap	Key Wrapping using AES-KW or AES-KWP	Security Strength:Key establishment methodology provides between 128 and 256 bits of encryption strength.	AES-KW AES-KWP

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

The following algorithm specific information applies to algorithms used by the module in the approved mode of operation.

SHA-1:

Per NIST SP 800-131A rev3, usage of the SHA-1 service as part of digital signature generation is disallowed in the approved mode of operation.

AES-GCM:

Per FIPS 140-3 IG C.H, the module implements deterministic IV construction as described in NIST SP 800-38D, section 8.2.1. The IV is constructed internally, and deterministically, with a length of 96 bits.

The module provides the AES-GCM service to the calling application in a manner compatible with the TLS v1.2 protocol per RFC5246 and using cipher suites listed in section 3.3.1 or NIST SP 800-52rev2.

The module explicitly ensures that the counter (the nonce_explicit part of the IV) does not exhaust the maximum number of possible values of 2^64-1 for a given session key. If this exhaustion condition is observed, the module returns an error indication to the calling application, which will then need to either abort the connection, or trigger a handshake to establish a new encryption key.

In the event Module power is lost and restored the calling application must ensure that any AES GCM keys used for encryption or decryption are re-distributed.

AES-XTS:

Per NIST SP 800-38E, the module implements the AES-XTS algorithm. Per IG A.9, AES-XTS is to be used for storage applications only. The module performs the required key uniqueness check (Key_1 =/= Key_2) before processing data with the AES-XTS keys.

The user shall enforce the length of the data unit used by any AES-XTS implementation does not exceed 2^20 blocks.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

The module's entropy source is located within the TOEPP, but outside the cryptographic boundary of the module. The module passively receives entropy based on request by the calling applications and exercises no control over the amount of quality of the obtained entropy. As such, there is *No assurance of the minimum strength of generated SSPs (e.g., keys).* By default, the module requests 256 bits of entropy per request.

2.9 Key Generation

When generating asymmetric keys, the module uses the direct output of its approved DRBG to generate random numbers and seeding material, per the guidance in NIST SP 800-133rev2, Section 5.

2.10 Key Establishment

The module implements the following approved key agreement methods:

- KAS-ECC-SSC - NIST SP 800-56A Rev. 3 (FIPS 140-3 IG D.F, Scenario 2, Path (1)
- KAS-FFC-SSC - NIST SP 800-56A Rev. 3 (FIPS 140-3 IG D.F, Scenario 2, Path (1)

While the module implements the protocol-specific KDFs in support of key agreement operations, the module only offers cryptographic services at the API-level to calling applications and does not implement full key agreement within the module boundary.

The module implements the following key transport method:

- KTS-IFC – NIST SP 800-56B Rev. 2 (FIPS 140-3 IG D.G, Key Encapsulation/Un-encapsulation)
- AES Key wrapping using AES-KW and KWP (FIPS 140-3 IG D.G, Key Wrapping/Unwrapping)

2.11 Industry Protocols

The module implements approved cryptography to support the following industry-specific protocols:

- IKEv1, IKEv2, SSH, TLS v1.2, MACsec

However, the module only offers cryptographic services to calling applications and does not contain full implementations of industry protocols.

No parts of the TLS protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	The module accepts data input through the input arguments of the API functions.
N/A	Data Output	The module produces data output through the parameters 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.

Table 10: Ports and Interfaces

As a software cryptographic toolkit, all of the module's interfaces are defined at the Software/Firmware Module Interface (SFMI). The FIPS-defined logical interfaces are mapped to specific calls via a well-defined API, with which the operator interacts.

The data output interface is inhibited when the module is performing self-tests, performing zeroisation, or while in an error state.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not implement an authentication mechanism. The operator role of Crypto Officer is assumed implicitly.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None

Table 11: Roles

The module only supports 1 role: Crypto Officer (CO). This role is assumed implicitly by the operator when performing an approved service.

4.3 Approved Services

The module performs the following approves services:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Data Encryption, Decryption	Encrypt or decrypt data	1 (return code)	Parameters, plaintext or ciphertext, key	Status, ciphertext or plaintext	Data Encryption Data Decryption	Crypto Officer - AES Key: W,E - AES GCM Key: W,E
Key Derivation Function	Perform key derivation using a key derivation function	1 (return code)	Parameters, key/password	Status, derived key	Key Derivation Function	Crypto Officer - KDF Secret: G,R - TLS Pre-Master Secret: G,R - TLS Master Secret: G,R - KBKDF Key: G,R - KBKDF Derived Key: W,E - KDF Derived Key: W,E
Deterministic Random Bit Generation	Generate random numbers with	1 (return code)	N/A	Status, random number	Deterministic Random Bit Generation	Crypto Officer - Entropy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	SP800-90A Rev 1					Input: W,E,Z - DRBG 'V' Value: W,E - DRBG 'C' Value: W,E - DRBG Seed: G,E,Z - DRBG Key: W,E
Digital Signature	Generate or verify RSA or ECDSA digital signatures	1 (return code)	Parameters, RSA / ECDSA keys, message	Status, digital signature	Digital Signature	Crypto Officer - RSA Public Key: W,E - RSA Private Key: W,E - ECDSA Public Key: W,E - ECDSA Private Key: W,E
Message Authentication	Generate or verify data integrity	1 (return code)	Parameters, message, key	Status, message authentication code	Message Authentication	Crypto Officer - AES GCM Key: W,E - AES CMAC Key: W,E - HMAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,E
Key Agreement	Perform key agreement primitives on behalf of the calling process (does not establish keys into the module)	1 (return code)	Parameters, DH/ECDH keys	Status, shared secret	Key Agreement ECC Key Agreement FFC	Crypto Officer - DH Public Key: W,E - DH Private Key: W,E - DH Shared Secret: G - ECDH Public Key: W,E - ECDH Private Key: W,E - ECDH Shared Secret: G
Key Generation	Generate and verify an asymmetric keypair and DH parameters	1 (return code)	Parameters	Status, keypair	Key Generation	Crypto Officer - RSA Public Key: G,R - RSA Private Key: G,R - ECDSA Public Key: G,R - ECDSA Private Key: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DH Public Key: G,R - DH Private Key: G,R - ECDH Public Key: G,R - ECDH Private Key: G,R
Key Transport	Transport CSPs	1 (return code)	Parameters, plaintext or ciphertext key, transport key(s)	Status, plaintext or ciphertext key	Key Transport	Crypto Officer - Key Transport Key: W,E
Key Wrapping	Wrap CSPs for Transport	1 (return code)	Parameters, plaintext or ciphertext key, transport key(s)	Status, plaintext or ciphertext key	Key Wrapping	Crypto Officer - AES Key: W,E
Message digest	Generate a message digest	1 (return code)	Parameters, Message	Status, Digest of the message	Message digest	Crypto Officer
Zeroize	Zeroize all SSPs procedurally by power cycling or unloading the module	Successful completion (Procedural)	N/A	N/A	None	Crypto Officer - AES Key: Z - AES GCM IV: Z - AES GCM Key: Z - AES CMAC Key: Z - HMAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - Entropy Input: Z - DRBG 'C' Value: Z - DRBG 'V' Value: Z - DRBG Seed: Z - DRBG Key: Z - RSA Public Key: Z - RSA Private Key: Z - ECDSA Public Key: Z - ECDSA Private Key: Z - DH Public Key: Z - DH Private Key: Z - DH Shared Secret: Z - ECDH Public Key: Z - ECDH Private Key: Z - ECDH Shared Secret: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Key Transport Key: Z - KDF Secret: Z - KDF Derived Key: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - KBKDF Key: Z - KBKDF Derived Key: Z
Perform Self-tests	Perform the module self-tests on demand	1 (return code)	N/A	Status	None	Crypto Officer
Show Status	Command the module to output it's current status	1 (return code)	Parameters	Status	None	Crypto Officer
Show module's versioning information	Command the module to output the module version	1 (return code)	Parameters	Status	None	Crypto Officer

Table 12: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Data Encryption, Decryption (TDES)	Encrypt or decrypt data using Triple-DES (Return code of '0' for non-approved service)	Triple-DES	Crypto Officer

Table 13: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not support loading of external software.

5 Software/Firmware Security

5.1 Integrity Techniques

The module verifies the integrity of all software components within the cryptographic boundary using an HMAC-SHA2-256-based integrity technique. The module computes the HMAC digest of the entire software package that represents the module and compares the result against a stored pre-computed digest.

The module's pre-operational integrity check is performed automatically at module power-up.

5.2 Initiate on Demand

The module integrity check can be performed on demand by the module operator by rebooting the host platform or by calling on-demand self-test service of the module.

5.3 Open-Source Parameters

The module is based on the open-source OpenSSL FIPS Provider, version 3.1.5.

The module was built using the following open-source compiler:

- GCC – Version 11.3.1 20221121 (Red Hat 11.3.1-4)

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The cryptographic module has control over its own SSPs.

The EOSv4 operating system used by the module's operational environment uses proper memory and process management to prevent unauthorized access to CSPs and uncontrolled modifications of SSPs while the module is in process space. The OS also ensures via process management that processes spawned by the module are owned by the module itself, and not by external processes/operators. The module does not persistently store SSPs.

7 Physical Security

The cryptographic module is a multi-chip standalone software module and does not include any physical components. Therefore, no physical security mechanisms or protections are implemented, and the section 7 requirements do not apply to the module.

8 Non-Invasive Security

The module does not claim any mitigations against non-invasive attacks. Additionally, there are no non-invasive attack mitigations outlined in Annex F of ISO/IEC 19790:2012.

Therefore, the section 8 requirements do not apply to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	System Memory	Dynamic
External	Calling Application	Dynamic

Table 14: Storage Areas

The table above lists the SSP storage areas implemented by the module. The module does not implement persistent storage of SSPs, and only stores keys temporarily in RAM, within the process space of the module.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SSP Input	External	RAM	Plaintext	Automated	Electronic	
SSP Output	RAM	External	Plaintext	Automated	Electronic	
SSP Output (Encrypted)	RAM	External	Encrypted	Automated	Electronic	Key Transport
SSP Input (Encrypted)	External	RAM	Encrypted	Automated	Electronic	Key Transport

Table 15: SSP Input-Output Methods

The table above lists the SSP Input-Output methods implemented by the module. The module only inputs or outputs SSPs using automated, electronic means to and from within the module TEOPP.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Reboot Host	Reboot	Memory is zeroized upon reboot	Operator Initiated (Procedural)
Module Unload	Module Unload	Module unloaded from memory	Operator Initiated (Procedural)
API Call	Zeroize function runs automatically as part of services that temporarily store SSPs	Runs cleanup routine, then frees all memory locations where SSPs are stored.	Automatic (Part of other operator initiated services)

Table 16: SSP Zeroization Methods

The module does not persistently store keys; therefore, all keys are held in the module's process space in volatile memory and are effectively zeroized upon reboot of the host platform. The zeroize API function can be invoked by the calling application and zeroizes all SSPs in the module storage space.

9.4 SSPs

The module supports the keys and other SSPs listed in the table below:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	AES Key (CBC, CFB, CTR, ECB)	128,192, 256 - 128,192, 256	Symmetric Key - CSP			Data Encryption Data Decryption
AES GCM IV	AES-GCM Initialization Vector	96 bits - -	Key Component - CSP			Data Encryption Data Decryption
AES GCM Key	AES-GCM Key	128,192, 256 - 128,192, 256	Symmetric Key - CSP			Data Encryption Data Decryption
AES CMAC Key	CMAC Key	128, 192, 256 - 128, 192, 256	Symmetric Key - CSP			Data Encryption Data Decryption
HMAC Key	Key used for HMAC Operations	≥ 112 bits - ≥ 112 bits	HMAC Key - CSP			Message Authentication
Entropy Input	Externally generated entropy used to seed the DRBG	128 - 256 bits - 128 - 256 bits	Entropy - CSP			Deterministic Random Bit Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG 'C' Value	Hash-DRBG State Value	440 bits - -	DRBG Internal State - CSP			Deterministic Random Bit Generation
DRBG 'V' Value	DRBG Internal State Value	128-256 bits - -	DRBG Internal State - CSP			Deterministic Random Bit Generation
DRBG Seed	DRBG Internal State Value	128 - 256 bits - 128 - 256 bits	DRBG Internal State - CSP			Deterministic Random Bit Generation
DRBG Key	DRBG Internal State Value	128 - 256 bits - 128 - 256 bits	DRBG Internal State - CSP			Deterministic Random Bit Generation
RSA Public Key	Public Key used for RSA operations	≥ 1024 bits - 96 to 256 bits	RSA Keypair - PSP	Digital Signature		Digital Signature
RSA Private Key	Private Key used for RSA operations	≥ 2048 bits - 112 to 256 bits	RSA Keypair - CSP	Digital Signature		Digital Signature
ECDSA Public Key	Public Key used for EC operations	256 to 521 bits - 128 to 256 bits	EC Keypair - PSP	Digital Signature		Digital Signature
ECDSA Private Key	Private Key used for EC operations	256 to 521 bits - 128 to 256 bits	EC Keypair - CSP	Digital Signature		Digital Signature
DH Public Key	DH Public Key	2048 – 8192 bits - 112 to 200 bits	DH Keypair - PSP	Key Agreement FFC		Key Agreement FFC
DH Private Key	DH Private Key	2048 – 8192 bits - 112 to 200 bits	DH Keypair - CSP	Key Agreement FFC		Key Agreement FFC
DH Shared Secret	DH Shared Secret	2048 – 8192 bits - 112 to 256 bits	DH Shared Secret - CSP		Key Agreement FFC	Key Agreement FFC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ECDH Public Key	ECDH Public Key	224 - 521 bits - 112 to 256 bits	ECDH Keypair - PSP	Key Agreement ECC		Key Agreement ECC
ECDH Private Key	ECDH Private Key	224 - 521 bits - 112 to 256 bits	ECDH Shared Secret - CSP	Key Agreement ECC		Key Agreement ECC
ECDH Shared Secret	ECDH Shared Secret	112 to 256 bits - 112 to 256 bits	ECDH Shared Secret - PSP		Key Agreement ECC	Key Agreement ECC
Key Transport Key	Key Transport Key	128 to 256 bits - 128 to 256 bits	Key Transport - CSP			Key Transport
KDF Secret	Secret used for KDF operations	≥ 112 bits - ≥ 112 bits	KDF Secret - CSP	Key Derivation Function Key Agreement ECC Key Agreement FFC		Key Derivation Function
KDF Derived Key	Key resulting from the module's SP 800-135rev1 KDFs	≥ 112 bits - ≥ 112 bits	KDF Key - CSP	Key Derivation Function		Key Derivation Function
TLS Pre-Master Secret	Shared Secret used for TLS session establishment	112 to 256 bits - 112 to 256 bits	KDF Secret - CSP			Key Derivation Function
TLS Master Secret	Master Secret used for TLS session	112 to 256 bits - 112 to 256 bits	KDF Secret - CSP			Key Derivation Function
KBKDF Key	Key used for key based key derivation	112 to 256 bits - 112 to 256 bits	KDF Key - CSP			Key Derivation Function
KBKDF Derived Key	Key resulting from the	≥ 112 bits - ≥ 112 bits	Symmetric Key - CSP	Key Derivation Function		Key Derivation Function

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	module's KBKDF					

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
AES GCM IV	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
AES GCM Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	AES GCM IV:Derived From
AES CMAC Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
HMAC Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
Entropy Input	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
DRBG 'C' Value	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	DRBG 'V' Value:Used With
DRBG 'V' Value	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	DRBG 'C' Value:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Seed	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
DRBG Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
RSA Public Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	RSA Private Key:Paired With
RSA Private Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	RSA Public Key:Paired With
ECDSA Public Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	ECDSA Private Key:Paired With
ECDSA Private Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	ECDSA Public Key:Paired With
DH Public Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	DH Private Key:Paired With
DH Private Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	DH Public Key:Paired With
DH Shared Secret	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	DH Public Key:Used With DH Private Key:Used With
ECDH Public Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module	ECDH Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Unload API Call	
ECDH Private Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	ECDH Public Key:Paired With
ECDH Shared Secret	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	ECDH Public Key:Used With ECDH Private Key:Used With
Key Transport Key	SSP Input SSP Output SSP Output (Encrypted) SSP Input (Encrypted)	RAM:Plaintext RAM:Encrypted External:Plaintext External:Encrypted	Until Reboot	Reboot Host Module Unload API Call	
KDF Secret	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	
KDF Derived Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	KDF Secret:Derived From
TLS Pre-Master Secret	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	TLS Master Secret:Used With
TLS Master Secret	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	TLS Pre-Master Secret:Derived From
KBKDF Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	KBKDF Derived Key:Used With
KBKDF Derived Key	SSP Input SSP Output	RAM:Plaintext External:Plaintext	Until Reboot	Reboot Host Module Unload API Call	KBKDF Key:Derived From

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

The module performs the following pre-operational self-test:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A5259)	HMAC-SHA2-256	KAT	SW/FW Integrity	status output	

Table 19: Pre-Operational Self-Tests

The pre-operational integrity self-test is performed after the module is instantiated, but before the module transitions to the approved mode of operation. The HMAC-SHA2-256 CAST is performed conditionally, before the integrity test, and therefore before the first operational use of the algorithm.

10.2 Conditional Self-Tests

The module performs the following conditional self-tests:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5259)	128 bits	KAT	CAST	Successful initialization of the module	Encrypt	Module Initialization
AES-ECB (A5259)	128 bits	KAT	CAST	Successful initialization of the module	Decrypt	Module Initialization
KDF SP800-108 (A5259)		KAT	CAST	Successful initialization of the module	KDF KAT	Module Initialization
KAS-FFC-SSC Sp800-56Ar3 (A5259)	p=2048, q=256	KAT	CAST	Successful initialization of the module	Computation of shared secret 'Z' (dhEphem)	Module Initialization
KAS-ECC-SSC Sp800-56Ar3 (A5259)	P-256	KAT	CAST	Successful initialization of the module	Computation of shared secret 'Z' (Ephemeral Unified)	Module Initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-5) (A5259)	P-256	PCT	PCT	Success or failure of service	Sign and Verify PCT	Keypair generation
RSA KeyGen (FIPS186-5) (A5259)	2048-bit	PCT	PCT	Success or failure of service	Sign and Verify PCT	Keypair generation
AES-XTS Testing Revision 2.0 (A5259)	Check to confirm Key1 ≠ Key2	Key Check	PCT	Success or failure of service	XTS Key Check Check to confirm Key1 ≠ Key2 Key check Critical Function Success or failure of service Per IG C.I	XTS Key entry
SHA-1 (A5259)	SHA-1	KAT	CAST	Successful initialization of the module	Hash and compare digest	Module Initialization
HMAC-SHA2-256 (A5259)	SHA2-256	KAT	CAST	Successful initialization of the module	Hash and compare digest	Module Initialization
SHA2-512 (A5259)	SHA2-512	KAT	CAST	Successful initialization of the module	Hash and compare digest	Module Initialization
SHA3-256 (A5259)	SHA3-256	KAT	CAST	Successful initialization of the module	Hash and compare digest	Module Initialization
SHA3-512 (A5259)	SHA3-512	KAT	CAST	Successful initialization of the module	Hash and compare digest	Module Initialization
TLS v1.2 KDF RFC7627 (A5259)	SHA2-256	KAT	CAST	Successful initialization of the module	KDF KAT	Module Initialization
HMAC-SHA2-256 (A5259)	HMAC-SHA2-256	KAT	CAST	Successful initialization of the module	MAC KAT	Module Initialization
KDF IKEv1 (A5259)	SHA2-256	KAT	CAST	Successful initialization of the module	KDF KAT	Module Initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF IKEv2 (A5259)	SHA2-256	KAT	CAST	Successful initialization of the module	KDF KAT	Module Initialization
KDF SSH (A5259)	AES-128, SHA2-256	KAT	CAST	Successful initialization of the module	KDF KAT	Module Initialization
KTS-IFC (A5259)	2048-bit, SHA2-256, Key Length 256-bits	KAT	CAST	Successful initialization of the module	Key encapsulation test per SP 800-56Brev2 and IG 10.3.A	Module Initialization
Counter DRBG (A5259)	AES-128	KAT	CAST	Successful initialization of the module	Instantiate, Reseed, and Generate - Combined KAT per IG 10.3.A	Module Initialization
Hash DRBG (A5259)	SHA2-256	KAT	CAST	Successful initialization of the module	Instantiate, Reseed, and Generate - Combined KAT per IG 10.3.A	Module Initialization
HMAC DRBG (A5259)	HMAC-SHA2-256	KAT	CAST	Successful initialization of the module	Instantiate, Reseed, and Generate - Combined KAT per IG 10.3.A	Module Initialization
ECDSA SigGen (FIPS186-5) (A5259)	P-256	KAT	CAST	Successful initialization of the module	Sign and Verify KAT	Module Initialization
RSA SigGen (FIPS186-5) (A5259)	2048-bit	KAT	CAST	Successful initialization of the module	Sign and Verify KAT	Module Initialization

Table 20: Conditional Self-Tests

Conditional CASTs are performed at module initialization, after the module integrity test, and before the first operational use of the algorithms. Pairwise consistency tests are performed conditionally upon generation of an asymmetric keypair.

DRBG CASTs combine the Instantiate, Reseed, and Generate tests in a single sweep per the guidance in IG 10.3.A, Resolution 7.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5259)	KAT	SW/FW Integrity	User initiated module reboot	On demand self-test service

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
AES-ECB (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
KDF SP800-108 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
KAS-FFC-SSC Sp800-56Ar3 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
KAS-ECC-SSC Sp800-56Ar3 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
ECDSA KeyGen (FIPS186-5) (A5259)	PCT	PCT	When ECDSA keypairs are generated	As part of the Digital Signature Service
RSA KeyGen (FIPS186-5) (A5259)	PCT	PCT	When RSA keypairs are generated	As part of the Digital Signature Service
AES-XTS Testing Revision 2.0 (A5259)	Key Check	PCT	User initiated module reboot	Perform Self-tests service
SHA-1 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
HMAC-SHA2-256 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
SHA2-512 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
SHA3-256 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
SHA3-512 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
TLS v1.2 KDF RFC7627 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
HMAC-SHA2-256 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
KDF IKEv1 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
KDF IKEv2 (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF SSH (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
KTS-IFC (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
Counter DRBG (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
Hash DRBG (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
HMAC DRBG (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
ECDSA SigGen (FIPS186-5) (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service
RSA SigGen (FIPS186-5) (A5259)	KAT	CAST	User initiated module reboot	Perform Self-tests service

Table 22: Conditional Periodic Information

The module can perform the periodic pre-operational, and conditional self-tests procedurally, on demand, by power cycling the host platform.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The module's error state.	POST or CAST failure	Reload / Reboot Module	return code: "0x0"

Table 23: Error States

Failure of any module self-test will cause the module to set an internal flag and transition to the error state. In the error state, all cryptographic functions are inhibited. The data output interface is also inhibited when the module is in the error state. Any further requests to the module for cryptographic services will cause the module to return an error indicator.

To recover from the error state, the host platform must be power cycled. Power cycling will cause the module to perform the pre-operational self-tests and transition to the approved mode of operation.

Optional statement - If the module self-tests continue to fail after rebooting, the CO should contact Arista Networks, Inc. for assistance.

10.5 Operator Initiation of Self-Tests

The module operator can initiate the pre-operational and conditional self-tests by power cycling the host platform.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The cryptographic module is distributed as part of Arista products, in the images accessible through the Arista software downloads portal. Products bundle together the operating system, applications, OpenSSL, and fips.so. While there is no need for the module to be built by the user at any point in time, it can be verified as the correct one by checking an unique version identifier, embedded into the module during the build process. The version identifier can be checked by issuing the following command:

objcopy --dump-section .rodata2=/dev/stdout $(openssl info -modulesdir)/fips.so && echo

The output of the above command should be:
e8271acdca4674621a29e55d83fdbfb8990fbeb56b1a6eaf34082e562e5261e1

11.2 Administrator Guidance

The module comes pre-configured on the Arista device and will perform approved services without any operator intervention.

11.3 Non-Administrator Guidance

The module only implements the crypto-officer role, which is implicitly assumed. Therefore, there is no separate guidance required for non-administrator usage of the module.

12 Mitigation of Other Attacks

The module implements mitigations against 2 types of timing attacks against digital signature services.

Digital signature timing attacks involve measuring either the total processing time of digital signature and RSA operations, or the differences in execution times of processes during cryptographic operations.
The module implements mitigations against 2 types of timing attacks.

Constant-time implementations:

Constant-time implementations regulate the execution time deltas between cryptographic operations to prevent an attacker from reverse-engineering sensitive data or cryptographic keys during processing.

Numeric blinding:

Numeric blinding uses random values during RSA processing. Those values act as a blinding factor preventing the attacker from determining which operation has been called and what processed data was via measuring the total execution time of the cryptographic operation.