Arista Networks, Inc.

Arista EOS Crypto Module v2.0

FIPS 140-2 Non-Proprietary Security Policy
Version 1.7

October 16, 2021

Copyright Notice

Copyright © 2021 Arista Networks, Inc.

This document may be freely reproduced in whole or part without permission and without restriction.

References

Reference	Full Specification Name
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-4]	Digital Signature Standard (DSS)
[FIPS 197]	Advanced Encryption Standard (AES)
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38E]	Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage
[SP 800-67 Rev.2]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-90A Rev.1]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-131A Rev.2]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
[SP 800-135 Rev. 1]	Recommendation for Existing Application-Specific Key Derivation Function

Table of Contents

1 Introduction

This document is the non-proprietary security policy for the Arista EOS Crypto Module, hereafter referred to as the Module.

The Module is a static software library providing a C-language application program interface (API) for use by other processes that require cryptographic functionality. The Module is classified by FIPS 140-2 as a software module, multi-chip standalone module embodiment. The physical cryptographic boundary is the general purpose computer on which the module is installed. The logical cryptographic boundary of the Module is the OpenSSL API file. The Module performs no communications other than with the calling application (the process that invokes the Module services).

The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	NA
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	NA

Table 1 – Security Level of Security Requirements

The Module’s software version for this validation is v2.0. This is a fork of the OpenSSL FIPS Object Module version 2.0.16 with Arista’s implementation of FIPS 186-4 key generation, SSH KDF and TLS KDF.

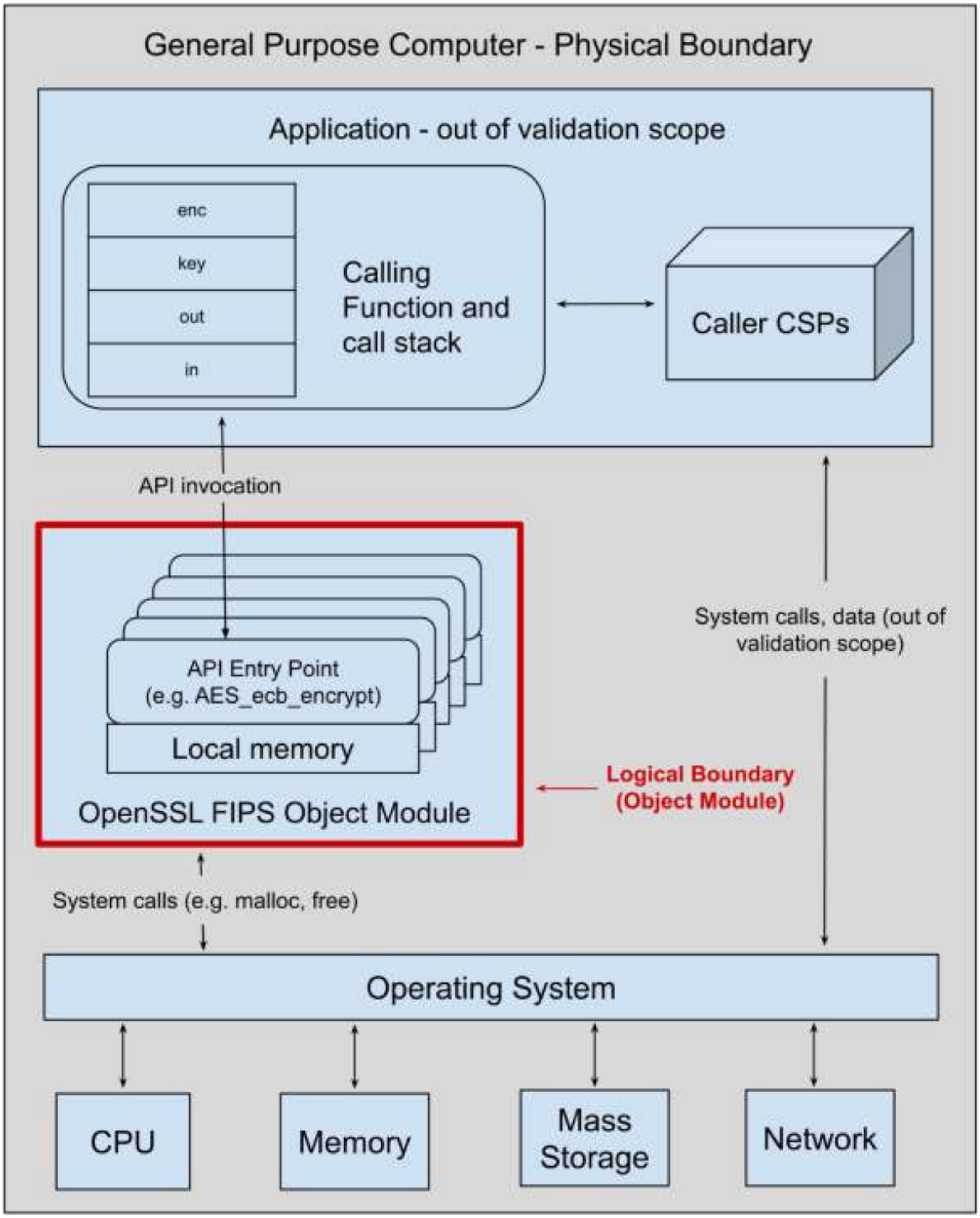
General Purpose Computer - Physical Boundary
Application - out of validation scope
enc
key
out
in
Calling Function and call stack
Caller CSPs
API invocation
API Entry Point (e.g. AES_ecb_encrypt)
Local memory
OpenSSL FIPS Object Module
Logical Boundary (Object Module)
System calls, data (out of validation scope)
System calls (e.g. malloc, free)
Operating System
CPU
Memory
Mass Storage
Network

Figure 1 - Module Block Diagram

2 Tested Configurations

#	Operational Environment	Processor
1	EOSv4 on Arista CCS-720XP-24Y6	AMD G-Series GX-224 (Crowned Eagle)
2	EOSv4 on Arista CCS-720XP-24ZY4	AMD G-Series GX-224 (Crowned Eagle)
3	EOSv4 on Arista CCS-720XP-48Y6	AMD G-Series GX-224 (Crowned Eagle)
4	EOSv4 on Arista CCS-720XP-48ZC2	AMD G-Series GX-224 (Crowned Eagle)
5	EOSv4 on Arista CCS-720XP-96ZC2	AMD R-Series RX-216 (Merlin Falcon)
6	EOSv4 on Arista CCS-750-Sup25	Intel Xeon D-1527 (Broadwell)

Table 2 - Tested Configurations

#	Operational Environment	Processor
1	EOSv4 on Arista CCS-750-Sup100	Intel Xeon D-1527 (Broadwell)
2	EOSv4 on Arista DCS-7050TX-128	Intel "Gladden" Sandy Bridge
3	EOSv4 on Arista DCS-7050TX-72	AMD eKabini GE420CIAJ44HM
4	EOSv4 on Arista DCS-7050TX-96	AMD eKabini GE420CIAJ44HM
5	EOSv4 on Arista DCS-7050CX3-32S	AMD Steppe Eagle GE424CIXJ44JB
6	EOSv4 on Arista DCS-7170-64C	Intel Broadwell-DE D1508
7	EOSv4 on Arista DCS-7020SR-32C2	Intel Broadwell DE D1508
8	EOSv4 on Arista DCS-7280SR3-40YC6	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
9	EOSv4 on Arista DCS-7280QRA-C36S	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
10	EOSv4 on Arista DCS-7280TR-48C6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
11	EOSv4 on Arista CCS-720XP-48Y6	AMD Crowned Eagle GX-224PC
12	EOSv4 on Arista CCS-720XP-24Y6	AMD Crowned Eagle GX-224PC
13	EOSv4 on Arista DCS-7060PX5-64	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
14	EOSv4 on Arista DCS-7150S-24-CL	AMD Athlon NEO X2 N40L
15	EOSv4 on Arista DCS-7050SX-128	Intel "Gladden" Sandy Bridge
16	EOSv4 on Arista DCS-7050QX-32S	AMD eKabini GE420CIAJ44HM
17	EOSv4 on Arista DCS-7050QX-32	AMD Athlon NEO X2 N40L
18	EOSv4 on Arista DCS-7050SX-64	AMD eKabini GE420CIAJ44HM
19	EOSv4 on Arista DCS-7050TX-48	AMD eKabini GE420CIAJ44HM

20	EOSv4 on Arista DCS-7050TX-64	AMD eKabini GE420CIAJ44HM
21	EOSv4 on Arista DCS-7050SX-72	AMD eKabini GE420CIAJ44HM
22	EOSv4 on Arista DCS-7050SX-96	AMD eKabini GE420CIAJ44HM
23	EOSv4 on Arista DCS-7280SE-72	AMD eKabini GE420CIAJ44HM
24	EOSv4 on Arista DCS-7280SE-64	AMD eKabini GE420CIAJ44HM
25	EOSv4 on Arista DCS-7010T-48	AMD eKabini GX-210HA or AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
26	EOSv4 on Arista DCS-7010T-48-DC	AMD eKabini GX-210HA or AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
27	EOSv4 on Arista DCS-7260QX-64	Intel "Gladden" Sandy Bridge
28	EOSv4 on Arista DCS-7280SE-68	AMD eKabini GE420CIAJ44HM
29	EOSv4 on Arista DCS-7050SX-72Q	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
30	EOSv4 on Arista DCS-7050TX-72Q	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
31	EOSv4 on Arista DCS-7050QX2-32S	AMD Steppe Eagle GE424CIXJ44JB
32	EOSv4 on Arista DCS-7050SX2-128	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
33	EOSv4 on Arista DCS-7050TX2-128	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
34	EOSv4 on Arista DCS-7280SR-48C6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
35	EOSv4 on Arista DCS-7280QR-C36	AMD Steppe Eagle GE424CIXJ44JB
36	EOSv4 on Arista DCS-7280CR-48	Intel "Gladden" Sandy Bridge
37	EOSv4 on Arista DCS-7160-48YC6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
38	EOSv4 on Arista DCS-7160-32CQ	AMD Steppe Eagle GE424CIXJ44JB
39	EOSv4 on Arista DCS-7260CX-64	Intel "Gladden" Sandy Bridge
40	EOSv4 on Arista DCS-7050SX2-72Q	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
41	EOSv4 on Arista DCS-7060CX-32S	AMD Steppe Eagle GE424CIXJ44JB
42	EOSv4 on Arista DCS-7060CX2-32S	AMD Steppe Eagle GE424CIXJ44JB
43	EOSv4 on Arista DCS-7160-48TC6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
44	EOSv4 on Arista DCS-7280QR-C72	Intel "Gladden" Sandy Bridge
45	EOSv4 on Arista DCS-7280SR2-48YC6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
46	EOSv4 on Arista DCS-7020TR-48	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
47	EOSv4 on Arista DCS-7280SR2A-48YC6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
48	EOSv4 on Arista DCS-7280SRA-48C6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
49	EOSv4 on Arista DCS-7280TRA-48C6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)

50	EOSv4 on Arista DCS-7020TRA-48	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
51	EOSv4 on Arista DCS-7280CR2A-60	Intel "Gladden" Sandy Bridge
52	EOSv4 on Arista DCS-7148SX	AMD Athlon NEO X2 N40L
53	EOSv4 on Arista DCS-7260CX3-64	Intel Broadwell-DE D1508
54	EOSv4 on Arista DCS-7280SRAM-48C6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
55	EOSv4 on Arista DCS-7060SX2-48YC6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
56	EOSv4 on Arista DCS-7280CR2K-60	Intel "Gladden" Sandy Bridge
57	EOSv4 on Arista DCS-7280CR2-60	Intel "Gladden" Sandy Bridge
58	EOSv4 on Arista DCS-7280CR2K-30	Intel Broadwell-DE D1508
59	EOSv4 on Arista DCS-7280CR2A-30	Intel Broadwell-DE D1508
60	EOSv4 on Arista DCS-7050SX3-48YC12	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
61	EOSv4 on Arista DCS-7280SR2K-48C6	AMD Steppe Eagle GX-424CC (GE424CIXJ44JB)
62	EOSv4 on Arista DCS-7170-32C	Intel Broadwell-DE D1508
63	EOSv4 on Arista DCS-7280SRM-40CX2	AMD Steppe Eagle GE424CIXJ44JB
64	EOSv4 on Arista DCS-7020SR-24C2	AMD Steppe Eagle GE424CIXJ44JB
65	EOSv4 on Arista DCS-7280CR2M-30	Intel Broadwell-DE D1508
66	EOSv4 on Arista DCS-7170-32CD	Intel Broadwell-DE D1508
67	EOSv4 on Arista CCS-720XP-48ZC2	AMD Crowned Eagle GX-224PC
68	EOSv4 on Arista DCS-7050SX3-48YC8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
69	EOSv4 on Arista CCS-720XP-24ZY4	AMD Crowned Eagle GX-224PC
70	EOSv4 on Arista DCS-7150SC-24-CLD	AMD Steppe Eagle GE424CIXJ44JB
71	EOSv4 on Arista DCS-7150SC-64-CLD	AMD Steppe Eagle GE424CIXJ44JB
72	EOSv4 on Arista DCS-7260CX3-64E	Intel Broadwell-DE D1508
73	EOSv4 on Arista DCS-7020SRG-24C2	AMD Steppe Eagle GE424CIXJ44JB
74	EOSv4 on Arista DCS-7060DX4-32	Intel Broadwell-DE D1508
75	EOSv4 on Arista DCS-7060PX4-32	Intel Broadwell-DE D1508
76	EOSv4 on Arista DCS-7280CR3-32P4	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
77	EOSv4 on Arista DCS-7280CR3K-32P4	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
78	EOSv4 on Arista DCS-7280PR3-24	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD

79	EOSv4 on Arista DCS-7280PR3K-24	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
80	EOSv4 on Arista DCS-7280CR3-32D4	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
81	EOSv4 on Arista DCS-7280CR3K-32D4	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
82	EOSv4 on Arista DCS-7050CX3M-32S	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
83	EOSv4 on Arista DCS-7280DR3-24	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
84	EOSv4 on Arista DCS-7280CR3-96	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
85	EOSv4 on Arista DCS-7280CR3K-96	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
86	EOSv4 on Arista DCS-7280CR3MK-32P4	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
87	EOSv4 on Arista DCS-7050TX3-48C8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
88	EOSv4 on Arista DCS-7050SX3-48C8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
89	EOSv4 on Arista DCS-7280DR3K-24	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
90	EOSv4 on Arista CCS-720XP-96ZC2	AMD R-Series RX-216 (Merlin Falcon)
91	EOSv4 on Arista DCS-7050SX3-96YC8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
92	EOSv4 on Arista DCS-7280CR3MK-32D4	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
93	EOSv4 on Arista DCS-7280SR3K-48YC8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
94	EOSv4 on Arista DCS-7280CR3MK-32D4S	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
95	EOSv4 on Arista DCS-7010TX-48	AMD Crowned Eagle GE224PIXJ23JB
96	EOSv4 on Arista DCS-7010TX-48-DC	AMD Crowned Eagle GE224PIXJ23JB
97	EOSv4 on Arista DCS-7280CR3MK-32P4S	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
98	EOSv4 on Arista DCS-7280SR3-48YC8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
99	EOSv4 on Arista DCS-7280CR3-36S	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD

100	EOSv4 on Arista DCS-7280CR3K-36S	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
101	EOSv4 on Arista DCS-7050DX4-32S	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
102	EOSv4 on Arista DCS-7050PX4-32S	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
103	EOSv4 on Arista DCS-7280CR3E-36S	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
104	EOSv4 on Arista DCS-7280CR3K-36A	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
105	EOSv4 on Arista DCS-7280SR3K-48YC8A	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
106	EOSv4 on Arista DCS-7280SR3M-48YC8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
107	EOSv4 on Arista DCS-7260CX3-64LQ	Intel Broadwell-DE D1508
108	EOSv4 on Arista DCS-7280SR3E-40YC6	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
109	EOSv4 on Arista DCS-7280CR3K-32D4A	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
110	EOSv4 on Arista DCS-7280CR3K-32P4A	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
111	EOSv4 on Arista DCS-7170B-64C	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
112	EOSv4 on Arista DCS-7132LN-48Y4C	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
113	EOSv4 on Arista DCS-7280DR3A-54	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
114	EOSv4 on Arista DCS-7280DR3AK-54	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
115	EOSv4 on Arista DCS-7280DR3AM-54	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
116	EOSv4 on Arista DCS-7280TR3-40C6	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
117	EOSv4 on Arista DCS-7060DX5-64	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
118	EOSv4 on Arista DCS-7280SR3E-48YC8	AMD Merlin Falcon R-series RX-421ND or AMD Merlin Falcon R-series RX-216TD
119	EOSv4 on Arista DCS-7135LB-48Y4C	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
120	EOSv4 on Arista DCS-7280CR3A-48D6	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
121	EOSv4 on Arista DCS-7280CR3AK-48D6	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
122	EOSv4 on Arista DCS-7280CR3AM-48D6	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
123	EOSv4 on Arista DCS-7132LB-48Y4CDC	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
124	EOSv4 on Arista DCS-7060PX5-64S	AMD Snowy Owl SP4r2 3151 or 3251 (4c or 8c)
125	EOSv4 on Arista 7368-SUP	Intel Xeon CPU D-1527
126	EOSv4 on Arista DCS-7516-SUP2	Intel Xeon CPU D-1548
127	EOSv4 on Arista DCS-7816-SUP	Intel Broadwell DE D-1548

128	EOSv4 on Arista CCS-750-SUP100	Intel Xeon D-1527 (Broadwell)
129	EOSv4 on Arista 7300-SUP	Intel Xeon CPU @ 2.60GHz
130	EOSv4 on Arista DCS-7500-SUP2	Intel Xeon CPU D-1528
131	EOSv4 on Arista DCS-7800-SUP	Intel Xeon CPU D-1528
132	EOSv4 on Arista DCS-7800-SUP1A	Intel Broadwell DE D-1528
133	EOSv4 on Arista CCS-750-SUP25	Intel Xeon D-1527 (Broadwell)
134	EOSv4 on Arista 7388-SUP	Intel Sandy Bridge Gladden AV8062701048500
135	SKN-7280CR3-4C2	Intel Broadwell-DE D1519
136	SKN-7280CR3-4C2G	Intel Broadwell-DE D1519
137	SKN-7280CR3-4C6	Intel Broadwell-DE D1519

Table 3 - Vendor Affirmed Configurations

The 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.

3 Ports and Interfaces

The physical ports of the Module are the same as the computer system on which it is executing. The logical interface is a C-language application program interface (API).

Logical interface type	Description
Control input	API entry point and corresponding stack parameters
Data input	API entry point data input stack parameters
Status output	API entry point return values and status stack parameters
Data output	API entry point data output stack parameters

Table 3 - Logical Interfaces

As a software module, control of the physical ports is outside module scope. However, when the module is performing self-tests, or is in an error state, all output on the logical data output interface is inhibited. The module is single-threaded and in error scenarios returns only an error value (no data output is returned).

4 Modes of Operation and Cryptographic Functionality

The Module supports only a FIPS 140-2 Approved mode and a non-Approved mode. The Approved mode is invoke by calling FIPS_mode_set() and using only Approved and allowed algorithms. Tables 4a and 4b list the Approved and non-approved but allowed algorithms, respectively.

Cert #	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
C1859	AES	FIPS 197, SP 800-38A	ECB, CBC, OFB, CFB-1, CFB-8, CFB-128	128, 192, 256	Encryption, Decryption
			CTR	128, 192, 256	Encryption
C1859	AES	SP 800-38B, SP 800-38C, SP 800-38D	CCM, GCM[1], CMAC, GMAC	128, 192, 256	Encryption, Decryption, Authentication
C1859	AES	SP 800-38E	XTS-AES[2]	128, 256	Confidentiality on storage devices only
Vendor Affirmed	CKG	SP 800-133	Unmodified output from the CTR_DRBG		Asymmetric Key Generation
C1859	CVL			2048	RSA Decryption Primitive
C1859	DRBG[3]	SP 800-90A	Hash_DRBG	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Random Bit Generation
			HMAC_DRBG		
			CTR_DRBG[4]	128, 192, 256	

C1859	DSA	FIPS 186-4		L=2048, N=224;
				L=2048, N=256;
				L=3072, N=256
					PQG and Key Generation

			SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	L=1024, N=160	Domain Parameter Verification
			SHA-224, SHA-256, SHA-384, SHA-512	L=2048, N=224	Domain Parameter Verification
			SHA-256, SHA-384, SHA-512	L=2048, N=256; L=3072, N=256	Domain Parameter Verification

			SHA-224, SHA-256, SHA-384, SHA-512	L=2048, N=224;
				L=2048, N=256;
				L=3072, N=256
					Signature Generation

			SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	L=1024, N=160;
				L=2048, N=224;
				L=2048, N=256;
				L=3072, N=256
					Signature Verification

C1859	ECDSA	FIPS 186-4		P-256, P-384, P-521	Key Generation

[1] GCM used in the context of TLS is compliant to IG A.5 if operator follows Operator Guidance in this document.

[2] XTS-AES is complaint to IG A.9 by checking for Key_1 ≠ Key_2 and shall only be used for storage application.

[3] For all DRBGs the "supported security strengths" is just the highest supported security strength per [SP800-90Ar1].

[4] The module uses CTR_DRBG by default.

Cert #	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
				P-256, P-384, P-521	Public Key Verification
			SHA-224, SHA-256, SHA-384, SHA-512	P-256, P-384, P-521	Signature Generation, Signature Generation Component
			SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	P-256, P-384, P-521	Signature Verification
C1859	HMAC	FIPS 198-1	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	112 bits or greater	Keyed Hash
C1859	CVL[5]	SP 800-135	SSHv2 KDF		Key Derivation
C1859	CVL[6]	SP 800-135	TLS KDF (v1.0/v1.1 and v1.2)		Key Derivation
C1859	RSA	FIPS 186-4	B.3.3, B.3.6	2048, 3072	Asymmetric Key Generation
			ANSI X9.31, PKCS 1.5, PKCSPSS SHA-224[7], SHA-256, SHA-384, SHA-512	2048. 3072	Digital Signature Generation
			ANSI X9.31, PKCS 1.5, PKCSPSS SHA-1, SHA-224[8], SHA-256, SHA-384, SHA-512	1024, 2048, 3072	Digital Signature Verification
		FIPS 186-2	ANSI X9.31 SHA-1, SHA-256, SHA-384, SHA-512	1024, 1536, 2048, 3072. 4096	Digital Signature Verification
			PKCS 1.5, PKCSPSS SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		
C1859	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digests
C1859	Triple-DES[9]	SP 800-67, SP 800-38A	TECB, TCBC, TCFB-1, TCFB-8, TCFB-64, TOFB	192	Encryption, Decryption
		SP 800-38B	CMAC	192	Authentication

Table 4a – FIPS Approved Cryptographic Functions

[5] Only the KDF to this protocol has been tested by CAVP. No parts of this protocol other than the KDF has been tested by the CAVP and CMVP.

[6] Only the KDF to this protocol has been tested by CAVP. No parts of this protocol other than the KDF has been tested by the CAVP and CMVP.

[7] ANSI X9.31 signature generation with SHA-224 has not been tested by CAVP.

[8] ANSI X9.31 signature verification with SHA-224 has not been tested by CAVP.

[9] Enforce 3-key encryption/decryption.

Category	Algorithm	Description
Key Wrapping[10]	RSA	PKCS#1-v1.5 padding is performed as shown in Section 8.1 of RFC 2313. The RSA algorithm may be used by the calling application for encryption or decryption of keys. It provides 112 or 128 bits of encryption strength. No claim is made for SP 800-56B compliance, and no CSPs are established across the module's physical boundary using these services.
Hashing	MD5 within TLS	Component of TLS KDF
Entropy	NDRNG	Entropy input to the Approved DRBGs

Table 4b – Non-FIPS Approved But Allowed Cryptographic Functions

The Module implements the following NIST-specified algorithms, which are non-Approved, either from algorithm transitions (e.g., SP 800-131A) or from not being tested:

Function	Algorithm	Options
Digital Signature and Asymmetric Key Generation	RSA (FIPS 186-2)	KeyGen, SigGen931, SigGenPKCS1.5, SigGenPSS
	DSA (L< 2048 or N < 224)	PQG Gen, Key Pair Gen, Sig Gen
Key Encryption, Decryption	RSA (modulo < 2048)	RSA key encryption/decryption
Key Agreement	EC Diffie-Hellman	Diffie-Hellman scheme using elliptic curve, supporting curves P-256, P-384, and P-521. This key agreement scheme provides between 128 and 256 bits of encryption strength; however, it is only a service provided for calling process use. It is not used to establish keys into the Module.

Table 4c – Untested and Transition-Disallowed Cryptographic Functions

The algorithms in Table 4c must not be used when operating in the FIPS mode of operation. The Module also implements the following algorithms, which are non-Approved:

Function	Algorithm	Function	Algorithm
Encryption and Decryption	AES/Triple-DES KW (non-compliant)	Encryption and Decryption	RC4
	Blowfish		RC5
	Camellia 128/192/256		SEED
	CAST5	Message Digest	MD4
	DES		MD5
	DES-X		RIPEMD-160
	IDEA		Whirlpool
	RC2	Keyed Hash	HMAC-MD5

Table 4d – Other non-Approved Cryptographic Functions

The algorithms in Table 4d are automatically disabled when in the FIPS mode of operation. The Module is a cryptographic engine library, which can be used only in conjunction with additional

[10] Non-SP 800-56B-complaint key transport using PKCS#1-v1.5 padding is allowed through 2023 per SP 800-131Ar2.

software. Aside from the use of the NIST defined elliptic curves as trusted third party domain parameters, all other FIPS 186 assurances are outside the scope of the Module, and are the responsibility of the calling process.

4.1 Critical Security Parameters and Public Keys

All CSPs used by the Module are described in this section. All access to these CSPs by Module services are described in Section 4. The CSP names are generic, corresponding to API parameter data structures.

Key	Description / Usage	Type	Storage	Entry	Destruction
RSA SGK	RSA (2048 or 3072) signature generation key	Asymmetric	Volatile memory only	Module API	Automatic or power cycle
RSA KDK	RSA (2048 or 3072) key decryption (private key transport) key	Asymmetric	Volatile memory only	Module API	Automatic or power cycle
DSA SGK	DSA (2048 or 3072) signature generation key	Asymmetric	Volatile memory only	Module API	Automatic or power cycle
ECDSA SGK	ECDSA (P-256, P-384 or P-521) signature generation key	Asymmetric	Volatile memory only	Module API	Automatic or power cycle
AES EDK	AES (128/192/256) encrypt / decrypt key	Symmetric	Volatile memory only	Module API	Automatic or power cycle
AES CMAC GVK	AES (128/192/256) CMAC generate / verify key	Symmetric	Volatile memory only	Module API	Automatic or power cycle
AES GCM EDK	AES (128/192/256) authenticated encrypt / decrypt key	Symmetric	Volatile memory only	Module API	Automatic or power cycle
AES XTS EDK	AES (128/256) encrypt / decrypt key	Symmetric	Volatile memory only	Module API	Automatic or power cycle
TDES EDK	TDES (3-Key) encrypt / decrypt key	Symmetric	Volatile memory only	Module API	Automatic or power cycle
TDES CMAC GVK	TDES (3-Key) CMAC generate / verify key	Symmetric	Volatile memory only	Module API	Automatic or power cycle
HMAC Key	Keyed hash key (160/224/256/384/512)	Symmetric	Volatile memory only	Module API	Automatic or power cycle
CTR_DRBG CSPs	V (128 bits) and Key (AES 128/192/256), entropy input (length dependent on security strength)	DRBG State	Volatile memory only	Module API	Automatic or power cycle
TLS Premaster Secret / Master Secret	TLS handshake	Symmetric	Volatile memory only	Module API	Automatic or power cycle
POST Keys	Hardcoded keys for power-up self-tests	N/A	Hardcoded into the module	N/A	N/A
Integrity Key	Software integrity test	N/A	Hardcoded into the module	N/A	N/A

Table 4.1a – Critical Security Parameters

CSP Name	Description
DSA SVK	DSA (1024/2048/3072) signature verification key
ECDSA SVK	ECDSA (P-256/P-384/P-521) signature verification key
RSA SVK	RSA (1024/2048/3072) signature verification public key
RSA KEK	RSA (2048/3072) key encryption (public key transport) key

Table 4.1b – Public Keys

For all CSPs and Public Keys:

Storage: RAM, associated to entities by memory location. The Module stores RNG and DRBG state values for the lifetime of the RNG or DRBG instance. The module uses CSPs passed in by the calling application on the stack. The Module does not store any CSP persistently (beyond the lifetime of an API call), with the exception of RNG and DRBG state values used for the Modules' default key generation service.

Generation: The Module implements SP 800-90A DRBG (Hash, HMAC, or CTR) services for generation of DSA, ECDSA, and RSA keys as shown in Table 4a. The calling application is responsible for storage of generated keys returned by the module.

Entry: All CSPs enter the Module's logical boundary in plaintext as API parameters, associated by memory location. However, none cross the physical boundary.
Output: The Module does not output CSPs or intermediate key generation values, other than as explicit results of key generation services. However, none cross the physical boundary.

Destruction: Zeroization of sensitive data is performed automatically by API function calls for temporarily stored CSPs. In addition, the module provides functions to explicitly destroy CSPs related to random number generation services. The calling application is responsible for parameters passed in and out of the module.

Private and secret keys are provided to the Module by the calling application, and are destroyed when released by the appropriate API function calls. Keys residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the Module defined API. The operating system protects memory and process space from unauthorized access. Only the calling application that creates or imports keys can use or export such keys. All API functions are executed by the invoking calling application in a non-overlapping sequence such that no two API functions will execute concurrently. An authorized application has access to all key data generated during the operation of the Module.

For operation in the Approved mode, Module users (the calling applications) shall use entropy sources that contain at least 112 bits of entropy. To ensure full DRBG strength, the entropy sources must meet or exceed the security strengths shown in the table below.

DRBG Type	Underlying Algorithm	Minimum Seed Entropy
Hash_DRBG or HMAC_DRBG	SHA-1	128
	SHA-224	192
	SHA-256	256
	SHA-384	256
	SHA-512	256

CTR_DRBG	AES-128	128
	AES-192	192
	AES-256	256

Table 4.1c – DRBG Entropy Requirements

The entropy source (NDRNG) of each tested configuration in Table 2 provides at least 7.246294 bits/byte of entropy. In the Approved mode the module uses 3072 bytes from the NDRNG to seed all DRBGs and all the DRBGs meet the minimum seed entropy in Table 4.1c.

5 Roles, Authentication, and Services

The Module implements the required User and Crypto Officer roles and does not perform operator authentication.

- User Role (User): Calling any of the API functions.
- Crypto Officer Role (CO): Installation of the Module and loading the Module on the host computer system

An operator implicitly assumes the role by calling the associated services in Table 3. All services implemented by the Module are listed below, along with a description of service CSP access. All services are available in both the Approved mode and the non-Approved mode. In the Approved mode, these services are restricted to the algorithms listed in Tables 4a and 4b. In the non-Approved mode, the algorithms listed in Tables 4c and 4d may also be used.

Service	Role	Description
Initialize	CO	Module initialization. Does not access CSPs.
Self-test	User	Perform self tests (FIPS_selftest). Does not access CSPs.
Show status	User	Functions that provide module status information: • Version (as unsigned long or const char *) • FIPS Mode (Boolean) Does not access CSPs.
Zeroize	User	Functions that destroy CSPs: • fips_drbg_uninstantiate: for a given DRBG context, overwrites DRBG CSPs (Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs.) All other services automatically overwrite CSPs stored in allocated memory. Stack cleanup is the responsibility of the calling application.
Random number generation	User	Used for random number and symmetric key generation. • Seed or reseed a DRBG instance • Determine security strength of a DRBG instance • Obtain random data Uses and updates Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs.
Asymmetric key generation	User	Used to generate DSA, ECDSA and RSA keys: RSA SGK, RSA SVK; DSA SGK, DSA SVK; ECDSA SGK, ECDSA SVK There is one supported security strength for each mechanism and algorithm type, the maximum specified in SP800-90
Symmetric encrypt/decrypt	User	Used to encrypt or decrypt data. Executes using any symmetric encryption key from Table 4.1a: AES EDK, AES CCM, AES GCM, Triple-DES EDK (passed in by the calling process).
Symmetric digest	User	Used to generate or verify data integrity with CMAC. Executes using AES CMAC, Triple-DES CMAC (passed in by the calling process).
Message digest	User	Used to generate a SHA-1 or SHA-2 message digest. Does not access CSPs.
Keyed hash	User	Used to generate or verify data integrity with HMAC. Executes using HMAC Key (passed in by the calling process).

Service	Role	Description
Key transport primitives[11]	User	Used to encrypt or decrypt a key value on behalf of the calling process (the key is treated as payload data; this service does not establish keys into the module). Executes using RSA KDK, RSA KEK (passed in by the calling process).
Key derivation	User	Used to perform key derivation primitives as per SP800-135: TLS KDF and SSH KDF (this service does not establish keys into the module).
Digital signature	User	Used to generate or verify RSA, DSA or ECDSA digital signatures. Executes using RSA SGK, RSA SVK; DSA SGK, DSA SVK; ECDSA SGK, ECDSA SVK (passed in by the calling process).
Utility	User	Miscellaneous helper functions. Does not access CSPs.

Table 5 - Services and CSP Access

[11] “Key transport” can refer to a) moving keys in and out of the module or b) the use of keys by an external application. The latter definition is the one that applies to the Module

6 Self-test

The Module performs the self-tests listed below on invocation of Initialize or Self-test.

Algorithm	Type	Test Attributes
Software integrity	KAT	HMAC-SHA-1
HMAC	KAT	One KAT per SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512
SHS	KAT	One KAT per SHA-1, SHA-256 and SHA-512
AES	KAT	Separate encrypt and decrypt, ECB mode, 128 bit key length
AES CCM	KAT	Separate encrypt and decrypt, 192 key length
AES GCM	KAT	Separate encrypt and decrypt, 256 key length
AES CMAC	KAT	CMAC generate and verify, 128, 192, 256 key lengths
Triple-DES	KAT	Separate encrypt and decrypt, ECB mode, 3-Key
Triple-DES CMAC	KAT	CMAC generate and verify, 3-Key
RSA	KAT	Sign and verify using 2048 bit key, SHA-256, PKCS#1
RSA DP	KAT	RSA decryption primitive using 2048 bit key
DSA	PCT	Sign and verify using 2048 bit key, SHA-384
DRBG	KAT	CTR_DRBG: AES-256 with and without derivation function Hash_DRBG: SHA-256 HMAC_DRBG: SHA-256
ECDSA	PCT	Sign, verify using P-224, P-384, K-233 and SHA512.
SSH KDF	KAT	SSH key derivation function
TLS KDF	KAT	TLS key derivation function

Table 6a - Power On Self Tests (KAT = Known answer test; PCT = Pairwise consistency test)

The `FIPS_mode_set()`[12] function performs all power-up self-tests listed above with no operator intervention required, returning a “1” if all power-up self-tests succeed, and a “0” otherwise. If any component of the power-up self-test fails an internal flag is set to prevent subsequent invocation of any cryptographic function calls. The module will only enter the FIPS Approved mode if the module is reloaded and the call to `FIPS_mode_set()` succeeds.

The power-up self-tests may also be performed on-demand by calling `FIPS_selftest()`, which returns a “1” for success and “0” for failure. Interpretation of this return code is the responsibility of the calling application.

[12] `FIPS_mode_set()` calls Module function `FIPS_module_mode_set()`

The Module also implements the following conditional tests:

Algorithm	Test
DRBG	Health Test as required by [SP800-90A] Section 11.3.3
DRBG	Continuous test (CRNGT) for stuck fault
NDRNG	Continuous test (CRNGT) for stuck fault
DSA	Pairwise consistency test on each generation of a key pair
ECDSA	Pairwise consistency test on each generation of a key pair
RSA	Pairwise consistency test on each generation of a key pair

Table 6b - Conditional Tests

Pairwise consistency tests are performed for both possible modes of use, e.g. Sign/Verify and Encrypt/Decrypt.

7 Operational Environment

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

8 Physical Security

The physical security requirements do not apply to the module. The module is a pure software module that executes on a general purpose computer.

9 Operator Guidance

9.1 Crypto Officer Guidance

Arista EOS Crypto Module, fipscanister.o, is distributed as a static object file. Crypto Officer shall check the sha-1 hash of the module matches 7e31c9aed2f39e41c9ae2bcb40fd67c36bf8a6d4 before linking the module into application or shared object.

9.2 User Guidance

User shall only use AES GCM within TLS 1.2 protocol using GCM ciphersuites from Section 3.3.1 of SP 800-52 Rev 1. User shall ensure the implementation of the nonce_explicit management logic inside the application outside the logical cryptographic boundary of the module shall ensure that when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key (e.g., a 64-bit counter starting from 0 and increasing, when it reaches the maximum value of 2^{64} - 1), either party (the client or the server) that encounters this condition triggers a handshake to establish a new encryption key – see Sections 7.4.1.1 and 7.4.1.2 in RFC 5246.

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.

User shall enforce the limit of 2^{20} 64-bit data block encryptions with the same three-key Triple-DES key applies when keys are generated as part of one of the recognized IETF protocols.

User shall enforce the limit of 2^{16} 64-bit data block encryptions with the same three-key Triple-DES key applies when key is not generated as part of a recognized IETF protocol.

User shall enforce the length of data unit for any instance of an implementation of XTS-AES does not exceed 2^{20} AES blocks.

10 Mitigation of other Attacks

The Arista EOS Crypto Module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for validation.