Dell OpenSSL Cryptographic Library v2.3, v2.4, and v2.5

FIPS 140-2 Non-Proprietary Security Policy

Document Revision 2.8

4/14/2021

Revision History

Revision	Date	Authors	Summary
0.1	06/23/2014	Ed Morris	Initial draft
0.2	07/22/2014	Ed Morris	Revised draft
0.3	07/28/2014	Ed Morris	Revised to include S5000 platform
0.4	08/04/2014	Ed Morris	Updates based upon feedback
0.5	09/22/2014	Ed Morris	Updated name
0.6	09/25/2014	Jan Provan	Updated to Dell Document Standards
0.7	09/29/2014	Jan Provan	Updated Product Names and aligned processor names throughout
0.8	10/10/2014	Ed Morris	Updated to remove leftover Gossamer templating and to incorporate Cygnacom/Jonathan's comments
0.9	10/27/2014	Jan Provan	Updated based on Jonathan's Comments
1.0	03/26/2105	Kevin Fowler	Updated to address items from CMVP Review
1.1	03/26/2015	Kevin Fowler	Updated for Module V2.2 FIPS validation on Dell EMC Networking OS 9.8(0.0) and additional S-series systems S3048, S4048.
1.2	05/06/2015	Jeff Yin	Updated table 2: corrected header row platform references, updated CAVP algorithm validation numbers
1.3	06/24/2015	Jeff Yin	Updated CAVP algorithm validation numbers, removed Z9000
1.4	06/30/2015	Jeff Yin	Minor quality updates
1.5	07/01/2015	Jeff Yin	Minor quality updates
1.6	12/03/2015	Jeff Yin	Updated to address items from CMVP Review
1.7	12/10/2015	Jeff Yin	Updated to address items from CMVP Review
1.8	06/23/2016	Jeff Yin	Updated for Module V2.4 FIPS validation on Dell EMC Networking OS 9.10(0.1) and additional systems: S3100, S6100-ON, C9010, Z9100-ON.
1.9	01/11/2017	Jeff Yin	Updated for Module v2.4 FIPS validation on Dell EMC Networking OS 9.11(0.0). Updated company name from "Dell Inc." and "Dell Networking" to "Dell EMC" and "Dell EMC Networking" where appropriate. Listed out explicit model names for S3100 series and revised names of "-ON" platforms. Updated © year to 2017.
2.0	08/01/2017	Jeff Yin	Updated for Module v2.4 FIPS validation on Dell EMC Networking OS 10.3.1.
2.1	8/22/2017	Jonathan Smith	Updated CAVP algorithm validation numbers
2.2	9/17/2018	Jeff Yin	Updated for Dell EMC Networking OS 9.12(1.0)
2.3	01/30/2019	Jonathan Smith	Updated for Dell EMC Networking OS 9.14(1.0)

2.4	04/19/2019	Jonathan Smith	Updated for v2.5 and Dell EMC Networking OS 10.4.3
2.5	06/14/2019	Jeff Yin	Added note in Operational Environments section surrounding FIPS 140-2 IG G.5.
2.6	01/06/2020	Jonathan Smith	Additional IG G.5 claim
2.7	04/09/2020	Paula Atchison	Updated for SmartFabric OS10, v10.5.0, algorithm listings and operational environments section.
2.8	4/14/21	Paula Atchison	Updated “Vendor Affirmed Operating Environments” section.

Table of Contents

Introduction

This non-proprietary FIPS 140-2 security policy for the Dell OpenSSL Cryptographic Library details the secure operation of the Dell OpenSSL Cryptographic Library as required in the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United State Department of Commerce. This document, the Cryptographic Module Security Policy, also referred to as the Security Policy, specifies the security rules under which the Dell OpenSSL Cryptographic Library must operate.

The Dell OpenSSL Cryptographic Library provides cryptography to Dell EMC Networking's Z-Series, S-Series, C9010, PowerEdge M1000e MXL and I/O Aggregator, PowerEdge FN I/O Module switches as well as other Dell Technologies products, providing them with the protection afforded by industry-standard, government-approved algorithms to ensure secure, remote management. Dell EMC Networking's switches leverage the Dell OpenSSL Cryptographic Library to ensure use of FIPS 140-2 validated cryptography.

Dell Cryptographic Library

The following sections describe the Dell OpenSSL Cryptographic Library.

Module Specification

The Dell OpenSSL Cryptographic Library (hereinafter referred to as the "Library," "cryptographic module," or the "module") is a software-only cryptographic module executing on a general-purpose computing system running Dell EMC Networking Operating System (OS). Version 2.3 of the cryptographic module runs on Dell EMC Networking OS 9.8(0.0), the module was updated to version 2.4 for Dell EMC Networking OS 9.10(0.1), Dell EMC Networking OS 9.11(0.0), Dell EMC Networking OS 9.12(1.0), Dell EMC Networking OS 9.14(1.0), as well as Dell EMC Networking OS 10.3.1, and the module was updated to version 2.5 for Dell EMC Networking OS 10.4.3 and Dell EMC Networking SmartFabric OS10, version 10.5.0.[1]

[1] Starting with the 10.5.0 release, "Dell EMC Networking OS" is known as "Dell EMC Networking SmartFabric OS10".

The physical perimeter of the general-purpose computing system comprises the module's physical cryptographic boundary, while the Dell OpenSSL Cryptographic Library constitutes the module's logical cryptographic boundary.

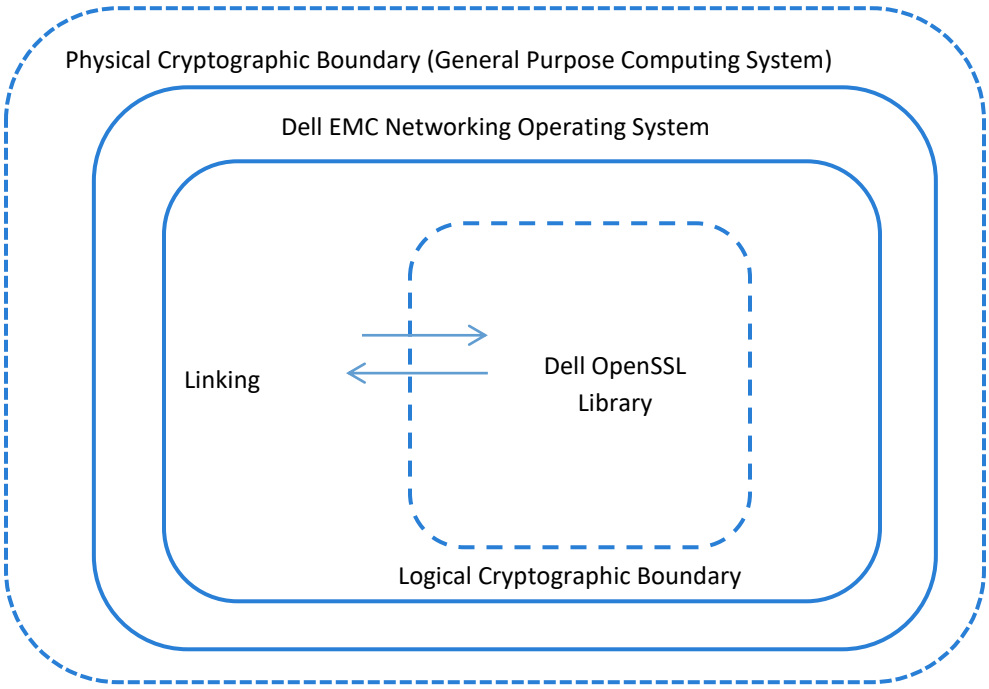

Figure 1 - Logical Diagram

Security Level

The Dell OpenSSL Cryptographic Library meets the overall requirements applicable to Level 1 security overall of FIPS 140-2 and the following specified section security levels.

Table 1 - Module Security Level Specification

#	FIPS 140-2 Section	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall Level	1

FIPS Approved Mode of Operation

The Dell OpenSSL Cryptographic Library provides both FIPS-Approved and non-FIPS-Approved services, and thus provides both a FIPS-Approved and non-Approved mode of operation. To use the Library in a FIPS-compliant mode of operation, the operator should following these rules:

1. As allowed by FIPS 140-2 overall Level 1 security, the module does not provide any indicator of its FIPS mode of operation. Thus, an operator (calling process) must ensure to follow each of the rules in this section (during the development of a calling application) to ensure that the module operates in its FIPS mode.
2. The module affords no persistent or permanent configuration to ensure use of its Approved mode or operation, rather the module, when in its operational state, alternates service by service between its Approved and non-Approved mode of operation (depending on what services the operator calls).
3. The list of services enumerated in the Roles, Services and Authentication section includes all security functions, roles, and services provided by the cryptographic module in both its Approved and non-Approved modes of operation.
4. An operator does *not* configure the module during power-up initialization to operate only in one mode or another mode. The module provides no such configuration, but instead requires the operator to only solicit Approved services and to not solicit non-Approved services. The following services are non-Approved services:
    a. Random Number Generation using ANSI X9.31 RNG (all non-compliant)
5. An operator must avoid violating Approved-mode key generation and usage requirements by:
    a. Not generating keys in a non-Approved mode of operation and then switch to an Approved-mode of operation (for example, using the ANSI X9.31 RNG to directly generate an AES encryption key for use in the Approved mode of Operation)
    b. Not electronically importing keys in plaintext in a non-Approved mode of operation and then switch to an Approved-mode of operation and use those keys for Approved services
    c. Not generating keys in an Approved-mode of operation and then switching to a non-Approved mode of operation and using the generated keys for non-Approved services
    d. Not changing the default RNG to non-approved ANSI X9.31 RNG algorithm via calls like ENGINE_set_RAND() and ENGINE_set_default_RAND(). When the module is in the Approved mode of operation, the default RNG is the validated AES-256 CTR_DRBG.
6. An operator must limit the use of Triple-DES per FIPS PUB 140-2 Implementation Guidance, Section A.13

a. When used with an IETF specified protocol, one key set must not be used to encrypt more than 2^{20} 64-bit data blocks.

b. When used general encryption, one key set must not be used to encrypt more than 2^{16} 64-bit data blocks.

7. An operator may use the following methods for construction of the AES GCM IV for encryption per FIPS PUB 140-2 Implementation Guidance, Section A.5. The selection of the IV construction method is the responsibility of the user of this module. The operator of the module must not use an externally generated IV.

   a. Construct the IV with the calling application within the module boundary for exclusive use with peer-to-peer industry standard protocols per FIPS PUB 140-2 Implementation Guidance, Section A.5 Key/IV Pair Uniqueness Requirements from SP 800-38D, Scenario #1.

      The module is compatible with TLSv1.2 and supports acceptable GCM ciphersuites from Section 3.3.1 of SP 800-52 Rev 1 or SP 800-52 Rev 2. TLSv1.2 protocol with AES GCM IV construction per RFC 5246 is supported with the counter set within the module boundary. When the IV is constructed according to TLS protocol, the IV must only be used within the context TLS protocol with AES GCM mode encryption. When the maximum number of possible values for a given session key is reached, a client hello or server hello should be sent to renegotiate security parameters per RFC 5246 or fail. In the event of power loss, a new AES GCM key must be established for the encryption function.

   b. For deterministic construction of AES GCM IV the IV must be constructed with the first 32 bits as a unique identifier (e.g. name of module) and use at least 32 bits as a deterministic non-repetitive counter for a combined IV length between 64 bits and 128 bits. The encryption of blocks must be aborted if the counter part of the IV exhausts the maximum number of possible values for a given encryption key. In the event of power loss, a new AES GCM key must be established for the encryption function.

8. An operator must limit the use of the XTS-AES mode of encryption/decryption per NIST SP 800-38E to data storage applications. The length of the data unit for any instance of an implementation of XTS-AES shall not exceed 2^{20} AES blocks. Key_1 and Key_2 must be established within the physical boundary as distinct values, the calling application shall ensure that Key_1 does not equal Key_2.

Approved Cryptographic Algorithms

The module uses cryptographic algorithm implementations that have received the following certificate numbers from the Cryptographic Algorithm Validation Program.

Table 2.1 – FIPS-Approved Algorithm Certificates for Dell EMC Networking OS 9.8(0.0)

Algorithm	CAVP Certificate (Dell EMC Networking OS 9.8(0.0) on FreeScale PowerPC e500, Intel Atom S1000, Intel Atom C2000, and Broadcom XLP)
AES	**#3440**
DRBG	**#839**
DSA	**#968**
HMAC	**#2189**
RSA	**#1761**
SHS	**#2840**
Triple-DES	**#1938**

Table 2.2 – FIPS-Approved Algorithm Certificates for Dell EMC Networking OS 9.10(0.1)

Algorithm	CAVP Certificate (Dell EMC Networking OS 9.10(0.1) on FreeScale PowerPC e500, Intel Atom S1000, Intel Atom C2000, Broadcom XLP, and ARM Cortex A9)
AES	**#4043**
DRBG	**#1210**
DSA	**#1094**
HMAC	**#2638**
RSA	**#2075**
SHS	**#3332**
Triple-DES	**#2210**

Table 2.3 – FIPS-Approved Algorithm Certificates for Dell EMC Networking OS 9.11(0.0)

Algorithm	CAVP Certificate (Dell EMC Networking OS 9.11(0.0) on FreeScale PowerPC e500, Intel Atom S1000, Intel Atom C2000, Broadcom XLP, and ARM Cortex A9)
AES	**#4320**
DRBG	**#1376**
DSA	**#1150**
HMAC	**#2853**
RSA	**#2334**
SHS	**#3556**
Triple-DES	**#2334**

Table 2.4 – FIPS-Approved Algorithm Certificates for Dell EMC Networking OS 9.12(1.0)

Algorithm	CAVP Certificate (Dell EMC Networking OS 9.12(1.0) on Intel Atom C2000)
AES	**#5673**
DRBG	**#2292**
DSA	**#1458**
HMAC	**#3775**
RSA	**#3052**
SHS	**#4544**
Triple-DES	**#2842**

Table 2.5 – FIPS-Approved Algorithm Certificates for Dell EMC Networking OS 9.14(1.0)

Algorithm	CAVP Certificate (Dell EMC Networking OS 9.14(1.0) on Intel Atom C2000 and ARM Cortex A9)
AES	**#C213**
DRBG	**#C213**
DSA	**#C213**
HMAC	**#C213**
RSA	**#C213**
SHS	**#C213**
Triple-DES	**#C213**

Table 2.6 – FIPS-Approved Algorithm Certificates for Dell EMC Networking OS 10.3.1

Algorithm	CAVP Certificate (Dell EMC Networking OS 10.3.1 on Intel Atom C2000)
AES	**#4718**
DRBG	**#1607**
DSA	**#1256**
HMAC	**#3135**
RSA	**#2571**
SHS	**#3863**
Triple-DES	**#2500**

Table 2.7 – FIPS-Approved Algorithm Certificates for Dell EMC Networking OS 10.4.3

Algorithm	CAVP Certificate (Dell EMC Networking OS 10.4.3 on Intel Atom C series)
AES	**#C616**
DRBG	**# C616**
DSA	**# C616**
HMAC	**# C616**
RSA	**# C616**
SHS	**# C616**
Triple-DES	**# C616**

Table 2.8 – FIPS-Approved Algorithm Certificates for Dell EMC Networking SmartFabric OS10, v10.5.0

Algorithm	CAVP Certificates -Dell EMC Networking SmartFabric OS10, v10.5.0	
	on Intel Atom C series	on Pentium D
AES	**#C1529**	**#C1530**
DRBG	**#C1529**	**#C1530**
DSA	**#C1529**	**#C1530**
ECDSA	**#C1529**	**#C1530**
HMAC	**#C1529**	**#C1530**
RSA	**#C1529**	**#C1530**
SHS	**#C1529**	**#C1530**
Triple-DES	**#C1529**	**#C1530**
CVL ECDH	**#C1529**	**#C1530**

Non-Approved Cryptographic Algorithms

The module uses the following non-FIPS 140-2 approved, but allowed, algorithms.

- RSA with 2048-bit to 16384-bit key sizes provides between 112 and 270 bits of encryption strength – allowed for use as part of a key-establishment scheme.
- Diffie-Hellman with 2048-bit to 16384-bit key sizes provides between 112 and 270 bits of encryption strength – allowed for use as part of a key-agreement scheme.
- Elliptic Curve Diffie-Hellman with 224, 256, 384, and 521-bit prime field sizes provides between 112 and 256 bits of encryption strength – allowed for use as part of a key-agreement scheme.

The module also provides the following non-Approved algorithms:

- ANSI X9.31 RNG (non-compliant)

As described above, in order to utilize the Library in FIPS-compliant mode, a calling process cannot solicit non-Approved algorithms.

Module Interfaces

The module is classified as a multiple-chip standalone module for FIPS 140-2 purposes. As such, the module's physical cryptographic boundary encompasses the general-purpose computing system running a Dell EMC Networking operating system (Dell EMC Networking OS or Dell EMC Networking SmartFabric OS10) and interfacing with the peripherals (through its console port, network (Ethernet and QSFP) ports, USB ports, and power adapter).

However, the module provides only a logical interface via an application programming interface (API) and does not interface with or communicate across any of the physical ports of the computing system. This logical interface exposes services that operators (calling applications) may use directly.

The module's C-language API interface provided by the module is mapped onto the four FIPS 140-2 logical interfaces: data input, data output, control input, and status output. It is through this logical API that the module logically separates them into distinct and separate interfaces. The mapping of the module's API to the four FIPS 140-2 interfaces is as follows:

- Data input – API entry point data input stack parameters
- Data output – API entry point data output stack parameters
- Control input – API entry point and corresponding stack parameters
- Status output – API entry point return values and status stack parameters

Roles, Services and Authentication

The module supports both of the FIPS 140-2 required roles, the Crypto-officer and the User role, and supports no additional roles. An operator implicitly selects the Crypto-officer role when loading (or causing loading of) the library and selects the User role when soliciting services from the module through its API. The module requires no operator authentication. The following table enumerates the module's services.

Table 3 - Service Descriptions for Crypto-officer and User Roles

Service	Description, Critical Security Parameter (CSP) and Key Access
Crypto-Officer services	
Library Loading	The process of loading the assembly
Self-test	Perform self-tests (FIPS_selftest)
User services	
Show Status	Functions that provide module status information • Version (an unsigned long or const char *) • FIPS Mode (Boolean) • FIPS POST Status (returns 1 if they failed)

Service	Description, Critical Security Parameter (CSP) and Key Access
	Does not access CSPs.
Zeroize	Functions that destroy CSPs: • fips_drbg_uninstantiate: for the DRBG context, overwrites DRBG CSPs All other services automatically overwrite CSPs stored in allocated memory. Stack cleanup is the responsibility of the calling application.
Random number generation	Used for random number generation. • Seed or reseed the DRBG instance • Determine security strength of the DRBG instance • Obtain random data Uses and updates the DRBG CSPs.
Asymmetric key generation	Used to generate RSA, DH, DSA, and EC keys: RSA Signature Generation Key (SGK), RSA Signature Verification Key (SVK), DH Private, DH Public, DSA SGK, DSA SVK, EC DH Private, EC DH Public, ECDSA SGK, ECDSA SVK There is one supported entropy strength for each mechanism and algorithm type, the maximum specified in SP 800-90A.
Symmetric encrypt/decrypt	Used to encrypt or decrypt data. For symmetric encryption or decryption, the module supports: • Approved AES: CBC, CCM, CFB1, CFB128, CMAC, CTR, ECB, GCM, OFB, or XTS modes • Approved Triple-DES: CBC, CFB8, CFB64, CMAC, ECB or OFB modes
Message digest	Used to generate a SHA-1 or SHA-2 message digest. Does not access CSPs.
Keyed Hash	Used to generate or verify data integrity with HMAC. Executes using HMAC Key (passed in by the calling process).
Key transport[2] primitives	Used to encrypt or decrypt a key value on behalf of the calling process (does not establish keys into the module). Executes using RSA Key Decryption Key (KDK), RSA Key Encryption Key (KEK) (passed in by the calling process).
Key agreement primitives	Used to perform key agreement primitives on behalf of the calling process (does not establish keys into the module). Executes using EC DH Private, DH Private, EC DH Public, DH Public (passed in by the calling process).
Digital Signature	Used to generate or verify RSA or DSA digital signatures. Executes using RSA Signature Generation Key (SGK), RSA Signature Verification Key (SVK); DSA SGK, DSA SVK,

[2] "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 OpenSSL FIPS Object Module

Service	Description, Critical Security Parameter (CSP) and Key Access
	ECDSA SGK, ECDSA SVK (passed in by the calling process).

Finite State Model

The module has a finite state model (FSM) that describes the module's behavior and transitions based on its current state and the command received. The module's FSM was reviewed as part of the overall FIPS 140-2 validation.

Physical Security

The physical security requirements does not apply to the module. The module is a software-only module that executes on a general-purpose computing system.

Operational Environment

The Library executes on a general-purpose operating system (Dell EMC Networking OS or Dell EMC Networking SmartFabric OS10) running in single-user mode that segregates processes into separate process spaces. Thus, the operating system separates each process space from all others, implicitly satisfying the FIPS 140-2 requirement for a single-user mode of operation.

Table 4.1 – Tested Operational Environments in Dell EMC Networking OS 9.8(0.0)

	Dell EMC Networking OS 9.8(0.0) (single-user mode) Executing on
1	Dell EMC Networking S3048-ON 1/10GbE top-of-rack switch with Intel Atom C2000
2	Dell EMC Networking S4048-ON 10/40GbE top-of-rack switch with Intel Atom C2000
3	Dell Networking S4810 10/40GbE top-of-rack switch with FreeScale PowerPC e500
4	Dell Networking S4820T 10GBASE-T/40GbE switch with FreeScale PowerPC e500
5	Dell EMC Networking S5000 10/40GbE top-of-rack switch with FreeScale PowerPC e500
6	Dell Networking S6000 10/40GbE top-of-rack switch with Intel Atom S1000
7	Dell Networking Z9500 Ethernet Fabric Switch with Intel Atom S1000
8	Dell EMC Networking MXL with Broadcom XLP
9	Dell PowerEdge M I/O Aggregator with Broadcom XLP
10	Dell PowerEdge FN I/O Module with Broadcom XLP

Table 4.2 – Tested Operational Environments in Dell EMC Networking 9.10(0.1)

	Dell EMC Networking OS 9.10(0.1) (single-user mode) Executing on
1	Dell EMC Networking S3048-ON 1/10GbE top-of-rack switch with Intel Atom C2000
2	Dell EMC Networking S4048-ON 10/40GbE top-of-rack switch with Intel Atom C2000
3	Dell Networking S4810 10/40GbE top-of-rack switch with FreeScale PowerPC e500
4	Dell Networking S4820T 10GBASE-T/40GbE switch with FreeScale PowerPC e500
5	Dell EMC Networking S5000 10/40GbE top-of-rack modular switch with FreeScale PowerPC e500
6	Dell Networking S6000 10/40GbE top-of-rack switch with Intel Atom S1000
7	Dell Networking Z9500 Ethernet Fabric Switch with Intel Atom S1000
8	Dell EMC Networking MXL with Broadcom XLP
9	Dell PowerEdge M I/O Aggregator with Broadcom XLP
10	Dell PowerEdge FN I/O Module with Broadcom XLP
11	Dell EMC Networking S3124 1/10GbE top-of-rack switch with ARM Cortex A9
12	Dell EMC Networking S3124F 1/10GbE top-of-rack switch with ARM Cortex A9
13	Dell EMC Networking S3124P 1/10GbE top-of-rack switch with ARM Cortex A9
14	Dell EMC Networking S3148 1/10GbE top-of-rack switch with ARM Cortex A9
15	Dell EMC Networking S3148P 1/10GbE top-of-rack switch with ARM Cortex A9
16	Dell EMC Networking S6100-ON 100GbE top-of-rack modular switch with Intel Atom C2000
17	Dell EMC Networking Z9100-ON 100GbE top-of-rack switch with Intel Atom C2000
18	Dell EMC Networking C9010 Network Director modular chassis switch with Intel Atom C2000
19	Dell EMC Networking S4048T-ON 10GBASE-T/40GbE top-of-rack switch with Intel Atom C2000
20	Dell EMC Networking S6010-ON 10/40GbE top-of-rack switch with Intel Atom C2000

Table 4.3 – Tested Operational Environments in Dell EMC Networking 9.11(0.0)

	Dell EMC Networking OS 9.11(0.0) (single-user mode) Executing on
1	Dell EMC Networking S3048-ON 1/10GbE top-of-rack switch with Intel Atom C2000
2	Dell EMC Networking S4048-ON 10/40GbE top-of-rack switch with Intel Atom C2000
3	Dell Networking S4810 10/40GbE top-of-rack switch with FreeScale PowerPC e500
4	Dell Networking S4820T 10GBASE-T/40GbE switch with FreeScale PowerPC e500
5	Dell EMC Networking S5000 10/40GbE top-of-rack modular switch with FreeScale PowerPC e500
6	Dell Networking S6000 10/40GbE top-of-rack switch with Intel Atom S1000
7	Dell Networking Z9500 Ethernet Fabric Switch with Intel Atom S1000
8	Dell EMC Networking MXL with Broadcom XLP
9	Dell PowerEdge M I/O Aggregator with Broadcom XLP
10	Dell PowerEdge FN I/O Module with Broadcom XLP
11	Dell EMC Networking S3124 1/10GbE top-of-rack switch with ARM Cortex A9
12	Dell EMC Networking S3124F 1/10GbE top-of-rack switch with ARM Cortex A9
13	Dell EMC Networking S3124P 1/10GbE top-of-rack switch with ARM Cortex A9
14	Dell EMC Networking S3148 1/10GbE top-of-rack switch with ARM Cortex A9
15	Dell EMC Networking S3148P 1/10GbE top-of-rack switch with ARM Cortex A9
16	Dell EMC Networking S6100-ON 100GbE top-of-rack modular switch with Intel Atom C2000
17	Dell EMC Networking Z9100-ON 100GbE top-of-rack switch with Intel Atom C2000
18	Dell EMC Networking C9010 Network Director modular chassis switch with Intel Atom C2000
19	Dell EMC Networking S4048T-ON 10GBASE-T/40GbE top-of-rack switch with Intel Atom C2000
20	Dell EMC Networking S6010-ON 10/40GbE top-of-rack switch with Intel Atom C2000

Table 4.4 – Tested Operational Environments in Dell EMC Networking 9.12(1.0)

	Dell EMC Networking OS 9.12(1.0) (single-user mode) Executing on
1	Dell EMC Networking S5048-ON 25/100GbE data center switch with Intel Atom C2000

Table 4.5 – Tested Operational Environments in Dell EMC Networking OS 9.14(1.0)

	Dell EMC Networking OS 9.14(1.0) (single-user mode) Executing on
1	Dell EMC Networking S3048-ON 1/10GbE top-of-rack switch with Intel Atom C2000
2	Dell EMC Networking S4048-ON 10/40GbE top-of-rack switch with Intel Atom C2000
3	Dell EMC Networking S4048T-ON 10GBASE-T/40GbE top-of-rack switch with Intel Atom C2000
4	Dell EMC Networking S5048-ON 25/100GbE data center switch with Intel Atom C2000
5	Dell EMC Networking S6010-ON 10/40GbE top-of-rack switch with Intel Atom C2000
6	Dell EMC Networking S6100-ON 100GbE top-of-rack modular switch with Intel Atom C2000
7	Dell EMC Networking Z9100-ON 100GbE top-of-rack switch with Intel Atom C2000
8	Dell EMC Networking C9010 Network Director modular chassis switch with Intel Atom C2000
9	Dell EMC Networking S3124 1/10GbE top-of-rack switch with ARM Cortex A9
10	Dell EMC Networking S3124F 1/10GbE top-of-rack switch with ARM Cortex A9
11	Dell EMC Networking S3124P 1/10GbE top-of-rack switch with ARM Cortex A9
12	Dell EMC Networking S3148 1/10GbE top-of-rack switch with ARM Cortex A9
13	Dell EMC Networking S3148P 1/10GbE top-of-rack switch with ARM Cortex A9

Table 4.6 – Tested Operational Environments in Dell EMC Networking OS 10.3.1

	Dell EMC Networking OS 10.3.1 (single-user mode) Executing on
1	Dell EMC Networking S3048-ON 1/10GbE top-of-rack switch with Intel Atom C2000
2	Dell EMC Networking S4048-ON 10/40GbE top-of-rack switch with Intel Atom C2000
3	Dell EMC Networking S4048T-ON 10GBASE-T/40GbE top-of-rack switch with Intel Atom C2000
4	Dell EMC Networking S6010-ON 10/40GbE top-of-rack switch with Intel Atom C2000
5	Dell EMC Networking S4128F-ON 10/100GbE top-of-rack switch with Intel Atom C2000
6	Dell EMC Networking S4128T-ON 10GBASE-T/100GbE top-of-rack switch with Intel Atom C2000
7	Dell EMC Networking S4148F-ON 10/100GbE top-of-rack switch with Intel Atom C2000
8	Dell EMC Networking S4148T-ON 10GBASE-T/100GbE top-of-rack switch with Intel Atom C2000
9	Dell EMC Networking S4148FE-ON 10/100GbE top-of-rack switch with long-range optics with Intel Atom C2000
10	Dell EMC Networking S4148U-ON 8GbFC/16GbFC/10GbE/100GbE top-of-rack switch with Intel Atom C2000

Table 4.7 – Tested Operational Environments in Dell EMC Networking OS 10.4.3

	Dell EMC Networking OS 10.4.3 (single-user mode) Executing on
1	Dell EMC Networking S3048-ON 1/10GbE top-of-rack switch with Intel Atom C Series
2	Dell EMC Networking S4048-ON 10/40GbE top-of-rack switch with Intel Atom C Series
3	Dell EMC Networking S4112F-ON 10/100GbE top-of-rack switch with Intel Atom C Series
4	Dell EMC Networking S4248FBL-ON 10/100GbE top-of-rack switch with Intel Atom C Series
5	Dell EMC Networking S5148F-ON 25/100GbE top-of-rack switch with Intel Atom C Series
6	Dell EMC Networking S5212F-ON 25/100GbE top-of-rack switch with Intel Atom C Series
7	Dell EMC Networking S6010-ON 10/40GbE top-of-rack switch with Intel Atom C Series
8	Dell EMC Networking Z9100-ON 100GbE top-of-rack switch with Intel Atom C Series
9	Dell EMC Networking Z9264F-ON 40/100GbE top-of-rack switch with Intel Atom C Series

Table 4.8 – Tested Operational Environments in Dell EMC Networking SmartFabric OS10, v10.5.0

	Dell EMC Networking SmartFabric OS10, v10.5.0 (single-user mode) Executing on
1	Dell EMC Networking S3048-ON 1/10GbE top-of-rack switch with Intel Atom C Series
2	Dell EMC Networking S4048T-ON 10/40GbE top-of-rack switch with Intel Atom C Series
3	Dell EMC Networking S4112T-ON 10/100GbE top-of-rack switch with Intel Atom C Series
4	Dell EMC Networking S4248FBL-ON 10/100GbE top-of-rack switch with Intel Atom C Series
5	Dell EMC Networking S5248F-ON 25/100GbE top-of-rack switch with Intel Atom C Series
6	Dell EMC Networking S6010-ON 10/40GbE top-of-rack switch with Intel Atom C Series
7	Dell EMC Networking Z9100-ON 100GbE top-of-rack switch with Intel Atom C Series
8	Dell EMC Networking Z9264F-ON 40/100GbE top-of-rack switch with Intel Atom C Series
9	Dell EMC Networking Z9332F-ON 400GbE top-of-rack switch with Intel Pentium D series

Vendor Affirmed Operating Environments

The Cryptographic Module Validation Program (CMVP) allows for porting of unmodified software cryptographic modules to compatible operating environments as described in Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program G.5, "Maintaining Validation Compliance of Software or Firmware Cryptographic Modules". The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys.

Summary of compatible Dell EMC Networking operational environment hardware platforms

- PowerSwitch S-series with Intel Atom C series processors
  - S3048-ON
  - S4048-ON
  - S4048T-ON
  - S4100-ON Series
    - S4112F-ON
    - S4112T-ON

        - S4128F-ON
        - S4128T-ON
        - S4148F-ON
        - S4148T-ON
        - S4148U-ON
        - S4148FE-ON
    - S4248FB-ON
    - S4248FBL-ON
    - S5200-ON Series
        - S5212F-ON
        - S5224F-ON
        - S5232F-ON
        - S5248F-ON
        - S5296F-ON
    - S6010-ON
- PowerSwitch N-series with Intel Atom C series processors
    - N3248TE-ON
- PowerSwitch Z-series with Intel Pentium D processors
    - Z9100-ON
    - Z9264F-ON
    - Z9332F-ON
- PowerSwitch Z-series with Intel Atom C series processors
    - Z9432F-ON
- PowerEdge MX-series with Intel Atom C series processors
    - MX5108n
    - MX9116n

All module versions in this security policy are considered validated, per IG G.5, running on Dell EMC Networking operating systems (Dell EMC Networking OS or Dell EMC Networking SmartFabric OS10) with supported platforms listed above.

Additionally the module may be ported to compatible general purpose computing operational environments that include x86 (64 bit) and ARMv7 processors, such as Dell EMC PowerEdge and/or other component systems. Compatible general purpose operating environments may include the following operating systems and hypervisors (if applicable):

- Dell EMC Isilon OneFS
- Dell EMC PowerScale OneFS
- Dell EMC PowerProtect Data Domain OS
- SUSE Linux Enterprise Edition
    - SLES 12 and service packs

    - SLES 15 and service packs
- CentOS Linux
    - CentOS 7
    - CentOS 8
- Amazon Linux
- CoreOS
- Debian 9
- FreeBSD 11 or 12 releases
- RancherOS
- Ubuntu 16 or 18 releases
- Windows 10
- Windows 10 IOT
- VMware
    - ESXi 5.5
    - ESXi 6
    - ESXi 6.5
    - ESXi 6.7
- Microsoft Hyper V
    - Windows Server 2012
    - Windows Server 2016
- KVM
    - Ubuntu 14.04
    - Ubuntu 16.04
    - RHEL 7.3
    - RHEL 7.2
    - SUSE 12-SP2
    - CentOS 7

All module versions in this security policy are considered validated, per IG G.5, running on any of the above general purpose operating environments.

Key Management

The module possesses its HMAC-SHA-1 self-integrity test key and power-up self-test known answer test (KAT) keys. Beyond those keys, the module does not store any other keys persistently. It is the calling applications responsibility to appropriately manage keys. The module can generate keys (DSA, EC, and RSA asymmetric key pairs), can accept keys entered by an operator, and affords an operator the ability to zeroize keys held in RAM.

Minimum Entropy Provided by Random Number Generation

When an approved DRBG is instantiated, it is seeded with 48 bytes (384 bits) from the entropy pool. Given that the lowest measured amount of entropy across all platforms was greater than 7 bits per byte of entropy, using a conservative estimate of 7 bits per byte of entropy yields 48 bytes * 7 bits/byte = 336 bits. Therefore, at the minimum, the approved DRBG can provide at least 336 bits of entropy per request.

The following table describes the module's security-relevant data items (SRDI's) including asymmetric and symmetric keys:

Table 5 - Module Security-Relevant Data Items

Key	Type	Bitsize	Description	Origin	Stored	Zeroized
RSA SGK	RSA	2048 or 3072	RSA PKCS#1, ANSI X9.31, or PSS signature generation key	Entered or Generated	RAM / plaintext	Clear method
RSA KDK	RSA	2048-16384	RSA key decryption (private key transport) key	Entered or Generated	RAM / plaintext	Clear method
DSA SGK	DSA	224 or 256	DSA signature generation key	Entered or Generated	RAM / plaintext	Clear method
ECDSA SGK	ECDSA	224-521	ECDSA signature generation key	Entered or Generated	RAM / plaintext	Clear method
DH Private	DH	224-512	DH private key agreement key	Entered or Generated	RAM / plaintext	Clear method
EC DH Private	EC DH	224-521	EC DH private key agreement key	Entered or Generated	RAM / plaintext	Clear method
AES EDK	AES	128-256	AES encrypt / decrypt key	Entered	RAM / plaintext	Clear method
Triple-DES EDK	Triple-DES	192	Triple-DES encrypt / decrypt key	Entered	RAM / plaintext	Clear method
HMAC Key	HMAC	112+	Keyed hash key intended for data integrity	Entered	RAM / plaintext	Clear method
CTR_DRBG Key	AES	256	AES-256 CTR_DRBG internal state Key	From environment	RAM /plaintext	Clear method
CTR_DRBG V (seed)	N/A	128	AES-256 CTR_DRBG internal state V (seed)	From environment	RAM /plaintext	Clear method
HASH_DRBG C	N/A	440 or 888	HASH_DRBG internal state C	From environment	RAM /plaintext	Clear method
HASH_DRBG V (seed)	N/A	440 or 888	HASH_DRBG internal state V (seed)	From environment	RAM /plaintext	Clear method
HMAC_DRBG Key	N/A	160-512	HMAC_DRBG internal state key	From environment	RAM /plaintext	Clear method
HMAC_DRBG V (seed)	N/A	160-512	HMAC_DRBG internal state V (seed)	From environment	RAM /plaintext	Clear method

The module also supports the following public/non-sensitive keys:

Table 6 - Module Public Keys

Key	Type	Bitsize	Description	Origin	Stored	Zeroized
RSA SVK	RSA	2048 or 3072	RSA PKCS#1, ANSI X9.31, or PSS signature verification key	Entered or Generated	RAM / plaintext	Clear method
RSA KEK	RSA	2048-16384	RSA key encryption (public key transport) key	Entered or Generated	RAM / plaintext	Clear method
DSA SVK	DSA	2048 or 3072	DSA signature verification key	Entered or Generated	RAM / plaintext	Clear method
ECDSA SVK	ECDSA	224-521	ECDSA signature verification key	Entered or Generated	RAM / plaintext	Clear method
DH Public	DH	2048-16384	DH public key agreement key	Entered or Generated	RAM / plaintext	Clear method
EC DH Public	EC DH	224-521	EC DH public key agreement key	Entered or Generated	RAM / plaintext	Clear method
Self-tests KAT Keys	All	All	Keys used for module Power-Up Known Answer Self-Test	Compiled into the module	Module image	N/A (see 140-2 IG 7.4)
Self-tests Integrity Keys	HMAC	256 bits	HMAC-SHA-1 key used by the module for its power up integrity test	Compiled into the module	Module image / plaintext & obfuscated	N/A (see 140-2 IG 7.4)

Electromagnetic Interference and Compatibility

The module meets Level 1 security for FIPS 140-2 EMI/EMC requirements as the Dell OpenSSL Cryptographic Library passed validation executing on a general-purpose computing system that confirms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (for example, for home use).

Self-Tests

The module provides the self-tests listed in Table 7.

Table 7 – Self-tests

FIPS Cryptographic Module Self-Tests
Power-Up Self-Tests
Integrity test (HMAC-SHA-1)
DRBG KAT (CTR_DRBG, HASH_DRBG, HMAC_DRBG - all applicable SP 800-90 Section 11 assurance tests)
SHA KATs (SHA-1, -224, -256, -384, -512)
HMAC-SHA KATs (SHA-1, -224, -256, -384, -512)
CMAC KATs
AES encrypt KAT and AES decrypt KAT
AES CCM KATs
AES GCM authenticated encryption KAT and AES GCM authenticated decryption KAT
AES XTS KATs
Triple-DES encrypt KAT and Triple-DES decrypt KAT
RSA sign KAT and RSA verify KAT
DSA sign KAT and DSA verify KAT
ECDSA Pairwise Consistency Test
Conditional Self-tests:
DSA Key Generation Pairwise Consistency Test
RSA Key Generation Pairwise Consistency Test
ECDSA Key Generation Pairwise Consistency Test
DRBG Continuous Random Number Generator Test
Seeding of DRBG Continuous Random Number Generator Test

The module automatically performs the complete set of power-up self-tests during library load to ensure proper operation, thus an operator has no access to cryptographic functionality unless the power-up self-tests passes and the library load succeeds. The power-up self-tests include an integrity check of the module's software using an HMAC-SHA-1 value calculated over the object module's in-memory image. Should the module fail a self-test, the module enters an Error state where it prohibits cryptographic services.

Additionally, the module performs both power-up and conditional self-tests for its cryptographic algorithms. An operator may invoke the power-up self-tests at any time by calling the FIPS Mode function.

Guidance and Secure Operation

The Dell OpenSSL Cryptographic Library meets overall Level 1 requirements for FIPS PUB 140-2. The following sections describe the Crypto-officer and User guidance.

Crypto-officer Guidance

The Crypto-officer or operator responsible for configuring the operational environment on which the module runs must ensure FIPS-compliant operation (as described in the section, *FIPS Approved Mode of Operation*, of the Security Policy).

Additionally, the Crypto-officer is defined to be the operator responsible for loading the library, thus when invoked by a calling application (either at library load or dynamically), the operating system loader loads the module, causing it to automatically perform its power-up self-tests. If the module fails its power-up self-tests, the module transitions into an Error state.

User Guidance

After the operating system has been properly configured by the Crypto-officer (if needed), the Dell OpenSSL Cryptographic Library requires the user to follow the rules of section *FIPS Approved Mode of Operation* in order to operate in a FIPS-compliant manner. Furthermore, the User must assume responsibility for managing all keys, as the module does not provide any persistent key storage.

Mitigation of Other Attacks

The Dell OpenSSL Cryptographic Library does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for validation.