Dell Crypto Library for Dell iDRAC and Dell OME-M v2.6

FIPS 140-2 Non-Proprietary Security Policy

Document Revision 1.0

July 28, 2022

Revision History

Revision	Date	Authors	Summary
1.0	July 28, 2022	Colby Harper	Module v2.6 FIPS validation for IDRAC and OME

Table of Contents

Introduction

This non-proprietary FIPS 140-2 security policy details the secure operation of the Dell Crypto Library for Dell iDRAC and Dell OME-M 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 Crypto Library must operate.

The Dell Crypto Library for Dell iDRAC and Dell OME-M provides cryptography to Dell iDRAC and Dell OME-M lifecycle controllers providing them with the protection afforded by industry-standard, government-approved algorithms to ensure secure, remote management. Dell iDRAC, Dell CMC, and Dell OME-M leverage the Dell Crypto Library for Dell iDRAC and Dell OME-M to ensure use of FIPS 140-2 validated cryptography.

Dell Cryptographic Library

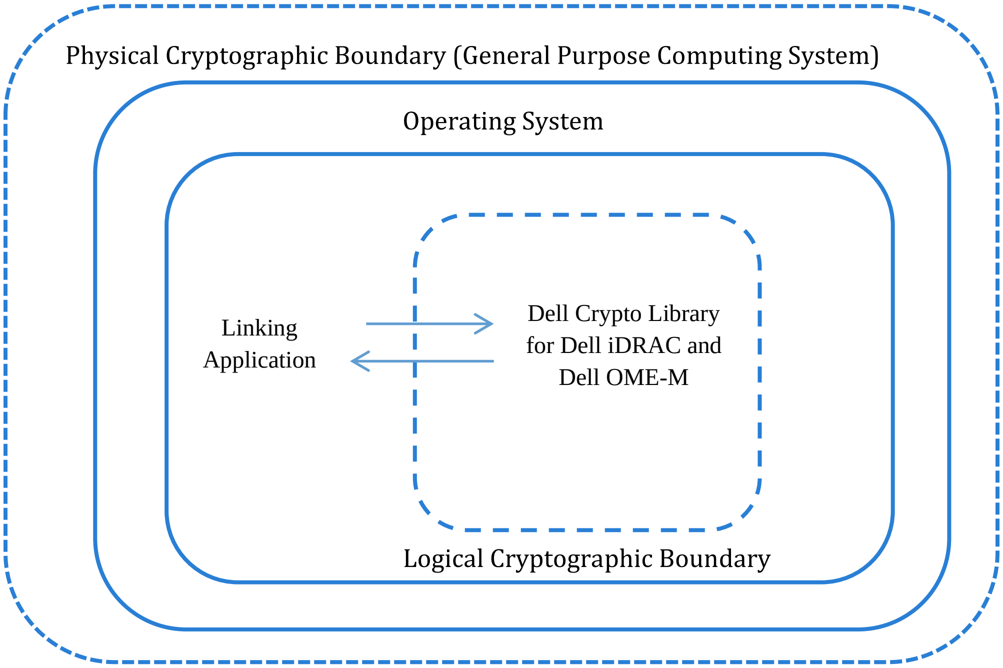
The following sections describe the Dell Crypto Library for Dell iDRAC and Dell OME-M.

Module Specification

The Dell Crypto Library for Dell iDRAC and Dell OME-M (hereinafter referred to as the “Library,” “cryptographic module,” or the “module”) is a software-only cryptographic module executing on a general-purpose computing system.

The physical perimeter of the general-purpose computing system comprises the module’s physical cryptographic boundary, while the Dell Crypto Library for Dell iDRAC and Dell OME-M constitutes the module’s logical cryptographic boundary.

Figure 1 - Logical Diagram



Security Level

The Dell Crypto Library for Dell iDRAC and Dell OME-M 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 Crypto Library for Dell iDRAC and Dell OME-M 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 must follow 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, Service 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)
    b. Triple-DES (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.
    e. When initializing Approved 800-90B DBRGs, users must consider the supported strength of the DRBG methods and the entropy source(s). The module supports DRBGs with varying length of required entropy input per NIST SP 800-90A. The length of the input string will depend on DRBG selected and desired security strength.

Module users shall provide, at a minimum, the “Minimum entropy input length” and entropy input that meets the security strength required for the random number generation mechanism as shown in SP 800-90A Table 2 (Hash_DRBG, HMAC_DRBG), and Table 3 (CTR_DRBG). The entropy input length may be equal to or greater than the target security strength of the DRBG based on the associated minimum entropy estimate (i.e. bits per byte) for the entropy input value. Per FIPS 140-2 I.G. 7.14, in all cases the minimum entropy input must contain at least 112 bits of entropy. The entropy is supplied by means of callback functions. The callback functions must return an error if the minimum entropy strength cannot be met.

6. 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. Note: The TLS protocol has not been reviewed or tested by the CAVP or CMVP.

    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.

7. 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.

8. When using Key agreement primitives (KAS-SSC), the operator shall ensure domain parameters are compliant to NIST SP 800-56A Rev. 3. NIST SP 800-56A rev.3 approved FFC

groups for KAS_SSC FFC (Diffie Hellman) provide between 112 and 200-bits of algorithm strength. NIST SP 800-56A rev.3 approved ECC curves for KAS_SSC ECC (Elliptic Curve Cryptography Diffie Hellman) provide between 112 and 256 bits of algorithm strength.

9. When using the supported RSA Key transport primitives, the module supports the allowed use of RSA key wrapping per FIPS 140-2 IG D.9. The RSA modulus must be at least 2048 bits. Only RSA PKCS#1-v1.5 padding consistent with RFC 2313, section 8.1 is allowed for use. Per FIPS 140-2 IG D.9 the use RSA key transport is disallowed for security relevant functions in the Approved Mode of Operation after December 31, 2023.

Approved Cryptographic Algorithms

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

Table 2 - FIPS-Approved Algorithms Certificates

Algorithms		CAVP Certificate
AES FIPS 197	SP800-38A • CBC (128, 192, 256) • CFB1 (128, 192, 256) • CFB128 (128, 192, 256) • CTR (128, 192, 256) • ECB (128, 192, 256) • OFB (128, 192, 256) SP800-38B • CMAC (128, 192, 256) SP800-38C • CCM (128, 192, 256) SP800-38D • GCM (128, 192, 256) SP900-38E • XTS (128, 256)	**A2213**

DRBG	SP 800-90A
	• COUNTER DRBG-AES 256
	• HASH DRBG
	  ○ SHA-1 or SHA-2 (224, 256, 384, 512)
	• HMAC DRBG
	  ○ SHA-1 or SHA-2 (224, 256, 384, 512)
		A2213

Algorithms		CAVP Certificate

DSA	FIPS 186-4
	• Key Pair Generation
	  ○ L/N: 2048/224, 2048/256, 3072/256
	• PQG Gen.
	  ○ L/N: 2048/224, 2048/256, 3072/256
	• PQG Ver.
	  ○ L/N: 1024/160, 2048/224, 2048/256, 3072/256)
	• Sign
	  ○ L/N: 2048/224, 2048/256, 3072/256
	  ○ SHA-2
	• Verify
	  ○ L/N: 1024/160, 2048/224, 2048/256, 3072/256)
	  ○ SHA-1 or SHA-2 (224, 256, 384, 512)
		A2213

ECDSA	FIPS 186-4
	• Key Pair Generation
	  ○ B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521
	• Key Verification
	  ○ B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521
	• Sign
	  ○ B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521
	  ○ SHA-2 (224, 256, 384, 512)
	• Verify
	  ○ B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521
	  ○ SHA-1 or SHA-2 (224, 256, 384, 512)
		A2213

HMAC	FIPS 198 SHA-1 SHA-2 (224, 256, 384, 512)	**A2213**
KAS-ECC-SSC (ECDH)	SP 800-56Ar3 Ephemeral Unified (B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521)	**A2213**
KAS-FFC-SSC (DH)	SP 800-56Ar3 dhEphem (2048, 3072, 4096, 6144, 8192)	**A2213**

	Algorithms	CAVP Certificate

RSA	FIPS 186-4
	• Key Pair Generation
	  ○ 2048, 3072
	• Sign
	  ○ 2048, 3072
	  ○ SHA-2 (224, 256, 384, 512)
	• Verify
	  ○ 2048, 3072
	  ○ SHA-2 (224, 256, 384, 512)
		A2213

SHS	FIPS 180-4 ○ SHA-1 or SHA-2 (224, 256, 384, 512)	**A2213**

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.

The module also provides the following non-Approved and not allowed algorithms:

- ANSI X9.31 RNG (non-compliant)
- Triple-DES (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 and Linux based OS 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) Does not access CSPs.
Zeroize	Functions that destroy CSPs: • fips_drbg_uninstantiate: for the DRBG context, overwrites DRBG CSPs

Service	Description, Critical Security Parameter (CSP) and Key Access
	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. The random value (seed) needed to generate an asymmetric key pair is the direct output of the Approved DRBG.
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
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[1] 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, DSA and ECDSA digital signatures. Executes using RSA Signature Generation Key (SGK), RSA Signature Verification Key (SVK); DSA SGK, DSA SVK, ECDSA SGK, ECDSA SVK (passed in by the calling process).

[1] "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

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 do 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 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 - Tested Operational Environments

	Tested OS and Processor
1	OME-M: Linux 4.9.241 on a PowerEdge MX7000 Modular Chassis w/ Dell OME-M with Intel Atom E3950
2	IDRAC: Linux 4.19.112 on a PowerEdge R750 Rack Server w/ Dell iDRAC9 with ARMv7 NPCMX50

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.

All module versions in this security policy are considered validated, per FIPS 140-2 IG G.5, running on a general-purpose computing platform and compatible operating system.

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.

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	Bit size	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	112-200*	DH private key agreement key	Entered or Generated	RAM / plaintext	Clear method
DH Z value	DH KAS	112-200*	DH KAS Shared secret Z Value	Agreement	RAM / plaintext	Clear method
EC DH Private	EC DH	112-256*	EC DH private key agreement key	Entered or Generated	RAM / plaintext	Clear method
EC DH Z value	EC DH KAS	112-256*	EC DH Shared secret Z Value	Agreement	RAM / plaintext	Clear method
AES EDK	AES	128-256	AES 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
* Key agreement: target security strength in bits per SP 800-56A Rev. 3 (rounded to nearest multiple of eight bits).						

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

Table 6 - Module Public Keys

Key	Type	Bit size	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	112-200*	DH public key agreement key	Entered or Generated	RAM / plaintext	Clear method
EC DH Public	EC DH	112-256*	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)
***** Key agreement: target security strength in bits per SP 800-56A Rev. 3 (rounded to nearest multiple of eight bits).						

Electromagnetic Interference and Compatibility

The module meets Level 1 security for FIPS 140-2 EMI/EMC requirements as the Dell Crypto Library for Dell iDRAC and Dell OME-M 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
RSA sign KAT and RSA verify KAT
DSA sign KAT and DSA verify KAT
ECDSA Pairwise Consistency Test
KAS-FFC-SSC KAT
KAS-ECC-SSC KAT
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 Crypto Library for Dell iDRAC and Dell OME-M 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 Crypto Library for Dell iDRAC and Dell OME-M 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 Crypto Library for Dell iDRAC and Dell OME-M does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for validation.