Dell Crypto Library for Dell iDRAC and Dell CMC v2.4

FIPS 140-2 Non-Proprietary Security Policy

Document Revision 1.0A

03/01/2017

Revision History

Revision	Date	Authors	Summary
1.0	01/18/2017	Kwok Wong	Modified from the OEM SP from 140-2 Cert. #2496

Table of Contents

Introduction

This non-proprietary FIPS 140-2 security policy for the Dell Crypto Library for Dell iDRAC and Dell CMC details the secure operation of the Dell Crypto Library for Dell iDRAC and Dell CMC 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 Crypto Library for Dell iDRAC and Dell CMC provides cryptography to Dell iDRAC and Dell CMC lifecycle controlers and provides them with the protection afforded by industry-standard, government-approved algorithms to ensure secure, remote management. Dell iDRAC and Dell CMC leverage the Dell Crypto Library for Dell iDRAC and Dell CMC 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 CMC.

Module Specification

The Dell Crypto Library for Dell iDRAC and Dell CMC (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 Linux 3.2.18 or Linux 3.4.11.

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 CMC constitutes the module's logical cryptographic boundary.

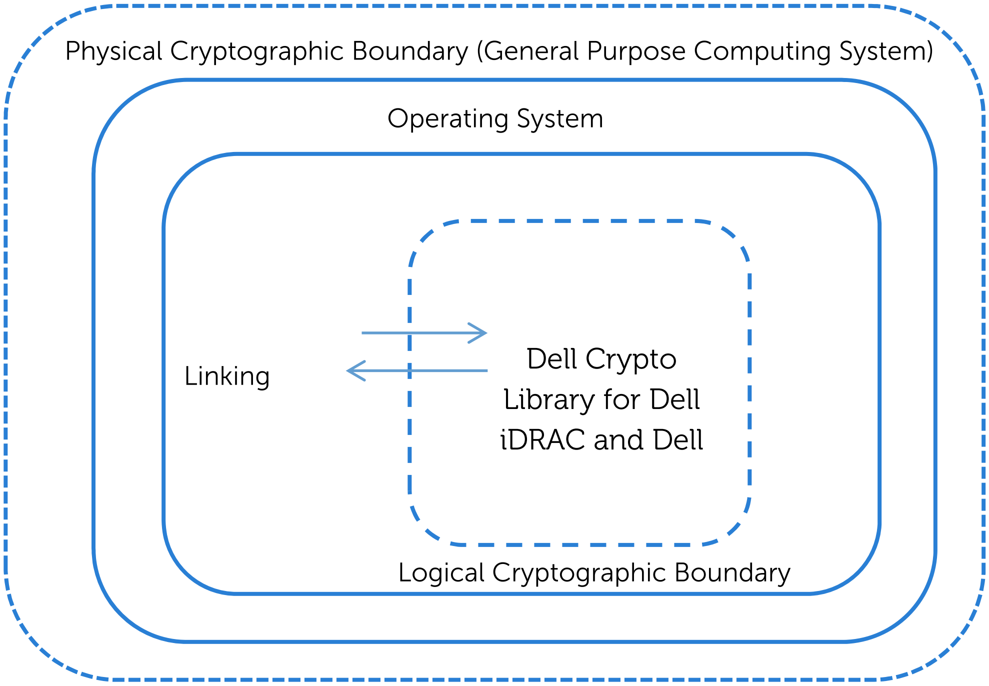
Physical Cryptographic Boundary (General Purpose Computing System)
Operating System
Linking
Dell Crypto Library for Dell iDRAC and Dell
Logical Cryptographic Boundary

Figure 1 - Logical Diagram

Security Level

The Dell Crypto Library for Dell iDRAC and Dell CMC 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 CMC 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 Hash_DRBG, HMAC_DRBG, and ANSI X9.31 RNG (all non-compliant)
    b. ECDSA (non-compliant)
    c. Triple-DES CMAC (non-compliant)
    d. AES CMAC (non-compliant), AES-GCM (non-compliant), and AES-XTS (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 same keys for the ECDH and ECDSA algorithms)

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 algorithms 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.

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 Algorithm Certificates

Algorithm	CAVP Certificate (Linux 3.2.18 on PowerPC 440EPX and Linux 3.4.11 on Renesas SH7758)
AES	**#4248**
DRBG	**#1327**
DSA	**#1138**
HMAC	**#2786**
RSA	**#2293**
SHS	**#3485**
Triple-DES	**#2303**

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:

- Hash_DRBG, HMAC_DRBG, and ANSI X9.31 RNG (non-compliant)
- ECDSA (non-compliant)
- Triple-DES CMAC (non-compliant)
- AES CMAC (non-compliant), AES-GCM (non-compliant), and AES-XTS (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 the Linux 3.2.18 or Linux 3.4.11 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 2 - Service Descriptions for Crypto-officer and User Roles

Service	Description and Critical Security Parameter (CSP) Access
Crypto-Officer services	
Library Loading	The process of loading the assembly
Self-test	Perform self-tests (FIPS_selftest)
User services	
Show Status	Fucntions 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 CTR_DRBG context, overwrites 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	Used for random number generation. • Seed or reseed the CTR_DRBG instance • Determine security strength of the CTR_DRBG instance • Obtain random data Uses and updates the CTR_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 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: ECB, CBC, CFB128, OFB, or CTR modes • Approved Triple-DES: ECB, CBC, CFB8, CFB64, or OFB modes

Service	Description and Critical Security Parameter (CSP) Access
	• Non-Approved AES CMAC, Triple-DES CMAC, AES-GCM, or AES-XTS
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 or DSA digital signatures. Executes using RSA Signature Generation Key (SGK), RSA Signature Verification Key (SVK); DSA SGK, DSA SVK (passed in by the calling process).

Finite State Model

The module has a finite state model (FSM) that descrbes 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 (Linux 3.2.18 or Linux 3.4.11) running in single-user mode that segregates processes into separate process spaces. Thus,

[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

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 3.1 – Tested Operational Environments in Dell iDRAC8

Linux 3.4.11 (single-user mode) Executing on	
1	PowerEdge R730 Rack Server with Renesas SH7758 CPU and Dell iDRAC8 firmware 2.41

Table 4.2 – Tested Operational Environments in Dell CMC

Linux 3.2.18 (single-user mode) Executing on	
1	PowerEdge M1000e Chassis with PowerPC 440EPX CPU and Dell CMC firmware 5.21

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 the approved AES-256 CTR_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 5.7 bits per byte of entropy, using a conservative estimate of 7 bits per byte of entropy yields 48 bytes * 5.7 bits/byte = 273 bits. Therefore, at the minimum, the approved AES-256 CTR_DRBG can provide at least 273 bits of entropy per request.

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

Table 4 - 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	2048 or 3072	DSA 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

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

Table 5 - 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
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 it's 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 Crypto Library for Dell iDRAC and Dell CMC 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 - 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 (CMAC is non-compliant)

AES encrypt KAT and AES decrypt KAT
AES CCM KATs
AES GCM authenticated encryption KAT and AES GCM authenticated decryption KAT (GCM is non-compliant)
AES XTS KATs (XTS is non-compliant)
Triple-DES encrypt KAT and Triple-DES decrypt KAT
RSA sign KAT and RSA verify KAT
DSA sign KAT and DSA verify KAT
Conditional Self-tests:
DSA Key Generation Pairwise Consistency Test
RSA Key Generation Pairwise Consistency Test
AES-256 CTR_DRBG Continuous Random Number Generator Test
Seeding of CTR_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 CMC 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 CMC 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 CMC does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for validation.