FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

July 2018

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Michael J Cooper

Dated: 2/8/2018

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Randy Latta

Dated: 2/8/2018

Director, Security Architecture and Risk Management
Communications Security Establishment

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3216	07/03/2018	SUSE Linux Enterprise Server 12 SP2 - NSS Cryptographic Module	SUSE, LLC	Software Version: 2.0
3217	07/03/2018	Thunder Series Application Delivery Controller TH3030S, TH4440S, TH6630S, and TH7440S	A10 Networks, Inc.	Hardware Version: TH-3030S, TH-4440S, TH-6630S and TH-7440S; Firmware Version: 4.1.1-P3
3218	07/03/2018	Mojo AirTight Sensor	Mojo Networks, Inc.	Firmware Version: 8.2.1
3219	07/05/2018	Accellion Cryptographic Module	Accellion, Inc.	Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16
3220	07/05/2018	KeyPair Cryptographic Module for OpenSSL	KeyPair Consulting Inc.	Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16
3221	07/09/2018	HYCU Cryptographic Library	HYCU, Inc.	Software Version: 1.0.0
3222	07/10/2018	HGST Ultrastar® SS200 TCG Enterprise SSD	HGST, a Western Digital brand	Hardware Version: P/Ns SDLL1HLR-076T-CF Version 1, SDLL1MLR-038T-CF Version 1, SDLL1CLR-020T-CF Version 1, SDLL1DLR-960G-CF Version 1, SDLL1DLR-480G-CF Version 1, SDLL1MLR-032T-CF Version 1, SDLL1CLR-016T-CF Version 1, SDLL1DLR-800G-CF Version 1 and SDLL1DLR-400G-CF Version 1; Firmware Version: X141 and X350
3223	07/10/2018	Apple Secure Key Store Cryptographic Module, v1.0	Apple Inc.	Hardware Version: 1.2[1], 2.0[2]; Firmware Version: SEPOS
3224	07/10/2018	AEDS Daemon	Space Systems Loral	Software Version: 1.0
3225	07/11/2018	Cisco ASA Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR4110-ASA-K9, FPR4120-ASA-K9, FPR4140-ASA-K9, FPR4150-ASA-K9, FPR9K-SM-24 (SM-24), FPR9K-SM-36 (SM-36) and FPR9K-SM-44 (SM-44); Firmware Version: 9.8
3226	07/11/2018	Blue Cedar Cryptographic Module	Blue Cedar	Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16
3227	07/12/2018	FortiGate-1200D[1], FortiGate-1500D[2], FortiGate-2000E[3] and FortiGate-2500E[4]	Fortinet, Inc.	Hardware Version: C1AC57 [1], C1AA64 [2], C1AF49 [3] and C1AF51 [4] with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: FortiOS 5.4, b9791, 170802 [1,2], FortiOS 5.4, b3145, 170602 [3,4]
3228	07/12/2018	HikSSL	Hangzhou Hikvision Digital Technology Co., Ltd.	Software Version: 1.0.0
3229	07/12/2018	REDCOM Encryption 140-2	REDCOM Laboratories, Inc.	Software Version: 3.0.1
3230	07/12/2018	Lexmark Crypto Core	Lexmark International Inc.	Software Version: 2.1
3231	07/12/2018	ProtectServer Internal Express 2 (PSI-E2)	Gemalto	Hardware Version: VBD-05, Version Code 0200; Firmware Version: 5.01.02

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3232	07/13/2018	Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, ASA 5585-X SSP-20, ASA 5585-X SSP-40 and ASA 5585-X SSP-60 Adaptive Security Appliances	Cisco Systems, Inc.	Hardware Version: ASA 5506-X[1][2], ASA 5506H-X[1][2], ASA 5506W-X[1][2], ASA 5508-X[1][3], ASA 5516-X[1][4], ASA 5525-X[1], ASA 5545-X[1], ASA 5555-X[1] and [ASA 5585-X SSP-10, ASA 5585-X SSP-20, ASA 5585-X SSP-40 and ASA 5585-X SSP-60][1][5] with [AIR-AP-FIPSKIT=][1], [ASA5506-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3], [ASA5516-FIPS-KIT=][4] and [ASA5585-X-FIPS-KIT][5]; Firmware Version: 9.8
3233	07/16/2018	Baxter Spectrum IQ Cryptographic Module	Baxter International Inc.	Software Version: 3.12.4
3234	07/17/2018	MPU5	Persistent Systems, LLC	Hardware Version: P/N WR-5100, Versions: 4.0.B, 4.1.B, 4.2.B, 4.2.C, 4.3.A, 4.3.B, 4.3.C, 4.3.D, 4.4.B, 4.4.C, 4.4.D, 4.5.C, 4.5.D; Tamper Evident Paint P/N PROD-007; Firmware Version: 19.3.2
3235	07/20/2018	ViPNet Common Crypto Core	Infotecs	Software Version: 2.0
3236	07/20/2018	Samsung BoringSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.2
3237	07/20/2018	Acme Packet 6300	Oracle Communications	Hardware Version: 6300; Firmware Version: E-CZ8.0.0
3238	07/23/2018	TCT Random Number Generator	TCL Communication Ltd.	Hardware Version: 2.3.1
3239	07/23/2018	TCT Crypto Engine	TCL Communication Ltd.	Hardware Version: 3.0.0
3240	07/24/2018	FortiGate-5001D Blade with FortiGate-5144C Chassis	Fortinet, Inc.	Hardware Version: Blade: C1AA92; Chassis: C1AB98; Front Filler Panel: PN P16708-01: thirteen; Rear Filler Panel: PN P16710-01: fourteen; with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: FortiOS 5.4, b9791, 170802
3241	07/25/2018	Brocade Fabric OS FIPS Cryptographic Module 8.2	Brocade Communications Systems LLC	Software Version: 8.2
3242	07/25/2018	Acme Packet 4600	Oracle Communications	Hardware Version: 4600; Firmware Version: E-CZ8.0.0
3243	07/25/2018	Standalone IMB	GDC Technology Limited	Hardware Version: GDC-IMB-v4; Firmware Version: 3.0, Security Manager Firmware Version 1.7.0
3244	07/25/2018	Acme Packet 1100 [1] and Acme Packet 3900 [2]	Oracle Communications	Hardware Version: 1100 [1] and 3900 [2]; Firmware Version: E-CZ 8.0.0
3245	07/25/2018	Acme Packet VME	Oracle Communications	Software Version: E-CZ 8.0.0
3246	07/25/2018	Cisco Firepower 4100 and Cisco Firepower 9300 Series	Cisco Systems, Inc.	Hardware Version: FPR4110[1], FPR4120[1], FRP4140[1], FRP4150[1], FPR9300-SM24[2], FPR9300-SM36[2] and FPR9300-SM44[2] with FIPS Kit (Cisco_TEL.FIPS_Kit), and opacity shield 69-100250-01[1] or 800-102843-01[2]; Firmware Version: 2.2

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3247	07/25/2018	Juniper Networks SRX345/SRX345-DUAL-AC with Junos 15.1X49-D110	Juniper Networks, Inc.	Hardware Version: SRX345, SRX345-DUAL-AC with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS-FIPS-MODE 15.1X49-D110
3248	07/27/2018	NITROX XL 1600-NFBE HSM Family	Cavium Inc.	Hardware Version: P/Ns CN1610-NFBE1-3.0-G, CN1620-NFBE1-3.0-G, CN1620-NFBE3-3.0-G, CN1610-NFBE1-2.0-G, CN1620-NFBE1-2.0-G, CN1620-NFBE3-2.0-G and FN1620-NFBE2-G; Firmware Version: CN16XX-NFBE-FW-2.3-180205
3249	07/27/2018	HID Global ActivID Applet Suite v2.7.4 on Gemalto TOPDLv2.1	HID Global and Gemalto	Hardware Version: NXP P60D144P VA (MPH149); Firmware Version: Gemalto TOPDLV2.1 (Filter04) and HID Global ActivID Applet Suite v2.7.4
3251	07/27/2018	Cisco Firepower 2100 Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FP2110, FP2120, FP2130, FP2140 with FIPS Kit (AIR-AP-FIPSKIT=) and opacity shield 69-100250-01; Firmware Version: 9.8