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

September 2016

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, 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: _____

Dated: 10/3/2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 30 OCT 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2732	09/01/2016	HGST Ultrastar He10 TCG Enterprise HDD	HGST, a Western Digital company	Hardware Version: P/Ns HUH721010AL5205 (0001), HUH721010AL4205 (0001), HUH721008AL5205 (0001) and HUH721008AL4205 (0001); Firmware Version: R308 (38)
2733	09/01/2016	NITROXIII CNN35XX-NFBE HSM Family	Cavium Inc.	Hardware Version: P/Ns CNL3560P-NFBE-G, CNL3560-NFBE-G, CNL3530-NFBE-G, CNL3510-NFBE-G, CNL3510P-NFBE-G, CNN3560P-NFBE-G, CNN3560-NFBE-G, CNN3530-NFBE-G and CNN3510-NFBE-G; Firmware Version: CNN35XX-NFBE-FW-1.1 build 01
2734	09/02/2016	Juniper Networks LN1000 Mobile Secure Router	Juniper Networks, Inc.	Hardware Version: P/Ns LN1000-V, JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS-FIPS 12.1X46-D40
2735	09/02/2016	Vormetric Data Security Manager Virtual Appliance Module	Vormetric, Inc.	Software Version: 5.3.0
2736	09/02/2016	Tanium Cryptographic Module	Tanium, Inc.	Software Version: 1.0
2737	09/02/2016	IBM® Security QRadar® SIEM	IBM Corporation	Hardware Version: 7.2 with FIPS Replacement Labels (Part Number: 00FK877) and FIPS Replacement Baffles (Part Number: 5YKKK); Firmware Version: 7.2
2738	09/07/2016	ACI-3002-S Controller	APCON, Inc.	Hardware Version: P/N ACI-3002-S, Version 1.0; Firmware Version: 5.07.1 build 106
2739	09/08/2016	Rajant BreadCrumb LX4-2495 and LX4-2954	Rajant Corporation	Hardware Version: LX4-2495, LX4-2954 with FIPS Kit: P/N 42540; Firmware Version: 11.4.0-FIPS
2740	09/08/2016	Rajant BreadCrumb ME4-2409	Rajant Corporation	Hardware Version: ME4-2409 with FIPS Kit: P/N 42540; Firmware Version: 11.4.0-FIPS
2741	09/08/2016	IBM Security Modular Extensible Security Architecture	IBM Security	Software Version: 5.3.1
2742	09/12/2016	Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0	Red Hat(R), Inc.	Software Version: 4.0
2743	09/13/2016	HiCOS PKI Applet and Taiwan eID Applet on Oberthur Technologies ID-One Cosmo V8	Chunghwa Telecom Co., Ltd. and Oberthur Technologies	Hardware Version: '0F'; Firmware Version: '5601'; Firmware Extension: '082371'
2744	09/13/2016	Samsung SCrypto	Samsung Electronics Co., Ltd.	Software Version: 1.0
2745	09/15/2016	Cisco Aironet 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access Points	Cisco Systems, Inc.	Hardware Version: 1532e[5], 1532i[5], 1552e[2], 1552i[2], 1572[4], 1602e[3], 1602i[3], 1702[4], 2602e[4], 2602i[4], 2702e[4], 2702i[4], 3502e[2], 3502i[2], 3602e[1,4], 3602i[1,4], 3602p[1,4], 3702e[1,4], 3702i[1,4] and 3702p[1,4] with AIR-RM3000M[1], Marvell 88W8364[2], Marvell 88W8763C[3], Marvell 88W8764C[4] and Qualcomm Atheros AES-128w10i[5]} with FIPS Kit: AIRLAP-FIPSKIT=, VERSION B0; Firmware Version: 8.0 MR3 with IC2M v2.0

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2746	09/16/2016	Samsung BoringSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.0
2747	09/16/2016	IDPrime MD 830-revB	Gemalto	Hardware Version: SLE78CFX3000PH; Firmware Version: IDCore30-revB - Build 06, IDPrime MD Applet version V4.3.5.D and MSPNP Applet V1.2
2748	09/16/2016	Cisco Catalyst 4506-E with Supervisor Cards (WS-X45-SUP7-E and WS-X45-Sup7L-E) and Line Cards (WS-X4748-RJ45-E and WS-X4748-RJ45V+E)	Cisco Systems, Inc.	Hardware Version: WS-C4506-E with Supervisor card [WS-X45-SUP7-E or WS-X45-SUP7L-E] and Line cards [WS-X4748-RJ45V+E and WS-X4748-RJ45-E]; Firmware Version: IOS-XE 3.7.0E
2749	09/19/2016	Dell SonicWALL TZ Series TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W and TZ 600	Dell Software, Inc.	Hardware Version: P/Ns 101-500403-56 Rev. A, 101-500404-55 Rev. A, 101-500405-56 Rev. A, 101-500406-55 Rev. A, 101-500411-57 Rev. A, 101-500412-56 Rev. A and 101-500413-57 Rev. A; Firmware Version: SonicOS v6.2.5
2750	09/19/2016	Dell SonicWALL NSA Series SM 9600, SM 9400, SM 9200, NSA 6600	Dell Software, Inc.	Hardware Version: P/Ns 101-500380-71 Rev. A (SM 9600), 101-500361-70 Rev. A (SM 9400), 101-500363-70 Rev. A (SM 9200), 101-500364-66 Rev. A (NSA 6600); Firmware Version: SonicOS v6.2.5
2751	09/19/2016	Dell SonicWALL NSA Series 2600, 3600, 4600, 5600	Dell Software, Inc.	Hardware Version: P/Ns 101-500362-63 Rev. A (NSA 2600), 101-500338-64 Rev. A (NSA 3600), 101-500365-64 Rev. A (NSA 4600), 101-500360-65 Rev. A (NSA 5600); Firmware Version: SonicOS v6.2.5
2752	09/21/2016	PTP 820C, PTP 820S, PTP 820N, PTP 820A, PTP 820G and PTP 820GX.	Cambium Networks, LTD	Hardware Version: PTP 820C, PTP 820S, PTP 820N, PTP 820A, PTP 820G, PTP 820GX, PTP820 TCC-B-MC: N000082H001, PTP820 TCC-B2: N000082H002, PTP820 TCC-B2-XG-MC: N000082H003, PTP820 RMC-B: N000082H004; Firmware Version: PTP820 Release 8.3
2753	09/21/2016	Sentry 3 FIPS Series USB Flash Drive	DataLocker, Inc.	Hardware Version: SENTRY04F, SENTRY08F, SENTRY16F, SENTRY32F and SENTRY64F; Firmware Version: 3.05
2754	09/22/2016	Christie IMB-S2 4K Integrated Media Block (IMB)	Christie Digital Systems Canada Inc.	Hardware Version: 000-102675-03; Firmware Version: 1.7.0-4209 and 2.0.0-4398
2755	09/26/2016	FireSphere 14600	iboss, Inc.	Hardware Version: FireSphere 14600_FIPS; Firmware Version: 8.2.0.10
2756	09/26/2016	FireSphere 7960	iboss, Inc.	Hardware Version: FireSphere 7960_FIPS; Firmware Version: 8.2.0.10
2757	09/26/2016	EMC Data Domain Crypto-C Micro Edition	EMC Corporation	Software Version: 4.0.1
2758	09/26/2016	HiKey PKI Token	Chunghwa Telecom Co., Ltd.	Hardware Version: HiKey3.0-BK; Firmware Version: HiKey COS V3.1
2759	09/26/2016	CryptoServer CSe	Utimaco IS GmbH	Hardware Version: P/N CryptoServer CSe Version 4.00.4.2; Firmware Version: Firmware Package Version 4.0.3.0
2760	09/27/2016	HPE XP7 Encryption Ready Disk Adapter (eDKA)	Hewlett Packard Enterprise Company	Hardware Version: P/N: eSCAS(WP820) or eSCAM(WP820) Version: B/A5, B/A6 or B/A7; Firmware Version: 02.09.28.00, 02.09.32.00 or 02.09.37.00
2761	09/27/2016	FIPS Crypto Module	Ionic Security Inc.	Software Version: 1.1