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

December 2015

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: Michael J Cooper

Dated: 4 Jan 2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature:

Dated: 4 Jan 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2479	12/01/2015	VMAX 6 Gb/s SAS I/O Module with Encryption from EMC	EMC Corporation	Hardware Version: 303-161-101B-05; Firmware Version: 2.13.39.00
2480	12/02/2015	Luna® PCI-e Cryptographic Module	SafeNet, Inc.	Hardware Version: VBD-05-0100, VBD-05-0101 and VBD-05-0103; Firmware Version: 6.2.1 and 6.2.5
2481	12/02/2015	Luna® PCI-e Cryptographic Module	SafeNet, Inc.	Hardware Version: VBD-05-0100, VBD-05-0101 and VBD-05-0103; Firmware Version: 6.2.1 and 6.2.5
2482	12/07/2015	DRAEGER WCM9113 802.11ABGN VG2	Draeger Medical Systems Inc.	Hardware Version: MS32018 Rev. 02; Firmware Version: VG2 with Bootloader version 1.7
2483	12/11/2015	CryptoComplyTM | Java	SafeLogic Inc.	Software Version: 2.2-fips
2484	12/14/2015	SUSE Linux Enterprise Server 12 - StrongSwan Cryptographic Module	SUSE, LLC	Software Version: 1.0
2485	12/14/2015	HiKey PKI Token	Chunghwa Telecom Co., Ltd.	Hardware Version: HiKey3.0-BK; Firmware Version: HiKey COS V3.0
2486	12/15/2015	Luna® Backup HSM Cryptographic Module	SafeNet Assured Technologies, LLC	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.7 and 6.10.9
2487	12/15/2015	Luna® G5 Cryptographic Module	SafeNet Assured Technologies, LLC.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.7 and 6.10.9
2488	12/15/2015	Luna® PCI-E Cryptographic Module and Luna® PCI-E Cryptographic Module for Luna® SA	SafeNet Assured Technologies, LLC.	Hardware Version: VBD-05, Version Code 0100, VBD-05, Version Code 0101, VBD-05, Version Code 0103; Firmware Version: 6.10.7 and 6.10.9
2489	12/15/2015	Luna® PCI-E Cryptographic Module and Luna® PCI-E Cryptographic Module for Luna® SA	SafeNet Assured Technologies, LLC.	Hardware Version: VBD-05, Version Code 0100, VBD-05, Version Code 0101, VBD-05, Version Code 0103; Firmware Version: 6.10.7 and 6.10.9
2490	12/15/2015	Cisco Catalyst 6506, 6506-E, 6509, 6509-E Switches with Wireless Services Module-2 (WiSM2)	Cisco Systems, Inc.	Hardware Version: (6506, 6506-E, 6509 and 6509-E) with WiSM2, CN56XX, WS-X6K-SLOT-CVR-E, WS-SVCWISM2FIPKIT= , [CVPN6500FIPS/KIT=, version D0] and one Supervisor Blade: (VS-S2T-10G, VS-S2T-10G-XL, VS-S720-10G-3C or VS-S720-10G-3CXL); Firmware Version: 8.0
2491	12/16/2015	FireEye CM Series: CM-4400, CM-7400, CM-9400	FireEye, Inc.	Hardware Version: CM-4400, CM-7400, CM-9400; Firmware Version: 7.6
2492	12/16/2015	FireEye EX Series: EX-3400, EX-5400, EX-8400, EX-8420	FireEye, Inc.	Hardware Version: EX-3400, EX-5400, EX-8400, EX-8420; Firmware Version: 7.6
2493	12/16/2015	FireEye FX Series: FX-5400, FX-8400	FireEye, Inc.	Hardware Version: FX-5400, FX-8400; Firmware Version: 7.6

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2494	12/16/2015	FireEye NX Series: NX-900, NX-1400, NX-2400, NX-4400, NX-4420, NX-7400, NX-7420, NX-7500, NX-10000, NX-9450, NX-10450	FireEye, Inc.	Hardware Version: NX-900, NX-1400, NX-2400, NX-4400, NX-4420, NX-7400, NX-7420, NX-7500, NX-10000, NX-9450, NX-10450; Firmware Version: 7.6
2495	12/15/2015	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-1.0 build 35
2496	12/16/2015	Dell OpenSSL Cryptographic Library	Dell, Inc.	Software Version: 2.3
2497	12/16/2015	Cisco Systems 2504, 7500, 8510 Wireless LAN Controllers and Cisco Catalyst 6807-XL Switch with Wireless Services Module-2 (WiSM2)	Cisco Systems, Inc.	Hardware Version: (2504, 7500, 8510 with CN56XX) and (6807-XL with WiSM2, CN56XX and one Supervisor Blade: [VS-S2T-10G, VS-S2T-10G-XL, VS-S720-10G-3C or VS-S720-10G-3CXL]); Firmware Version: 8.0
2498	12/17/2015	Aruba AP-214, AP-215, AP-274, AP-275 and AP-277 Wireless Access Points	Aruba Networks, Inc.	Hardware Version: AP-214-F1, AP-215-F1, AP-274-F1, AP-275-F1 and AP-277-F1 with FIPS kit 4011570-01; Firmware Version: ArubaOS 6.4.3-FIPS
2500	12/18/2015	Luna® G5 Cryptographic Module	SafeNet Assured Technologies, LLC.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.7 and 6.10.9
2501	12/18/2015	HP BladeSystem c-Class Virtual Connect Module	Hewlett Packard Enterprise Development LP	Firmware Version: 4.41
2502	12/18/2015	BlackBerry Cryptographic Java Module	BlackBerry Limited	Software Version: 2.8 [1], 2.8.7 [2], 2.8.8 [3]
2503	12/18/2015	Harris AES Load Module	Harris Corporation	Firmware Version: R06A02
2504	12/18/2015	Security Builder FIPS Java Module	Certicom Corp.	Software Version: 2.8 [1], 2.8.7 [2], 2.8.8 [3]
2505	12/21/2015	Cisco FIPS Object Module	Cisco Systems, Inc.	Software Version: 6.0
2506	12/21/2015	HP P-Class Smart Array Gen9 RAID Controllers	Hewlett Packard Enterprise Development LP	Hardware Version: P244br, P246br, P440, P441, and P741m; Firmware Version: 2.52
2507	12/21/2015	Samsung Flash Memory Protector V1.0	Samsung Electronics Co., Ltd.	Software Version: 1.1; Hardware Version: 3.0
2508	12/22/2015	Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive (AL14SEQ model)	Toshiba Corporation	Hardware Version: A0 with AL14SEQ18EPB, AL14SEQ12EPB, AL14SEQ09EPB, AL14SEQ18EQB, AL14SEQ12EQB, AL14SEQ09EQB; Firmware Version: 0101
2509	12/22/2015	HP OpenCall HLR Cryptographic Module	Hewlett Packard®, Enterprise.	Software Version: I-HSS 01.08.01

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2510	12/23/2015	iEngine SSID Applet on Athena SCS IDProtect Duo for SLE78	Athena SCS, Inc.	Hardware Version: Infineon SLE78CLFX4000P P-MCC8-2-6 package; Firmware Version: Athena IDProtect 0302.0306.0004 with iEngine SSID Applet V1.0.2
2511	12/24/2015	Cisco Integrated Services Router (ISR) 4351 and 4331 (with SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P, PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) and Cisco Integrated Services Router (ISR) 4321 (with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256)	Cisco Systems, Inc.	Hardware Version: ISR 4351 [1], ISR 4331 [2] and ISR 4321 [3] with SM-ES3X-16-P [1,2], SM-ES3X-24-P [1,2], SM-D-ES3X-48-P [1,2], PVDM4-32 [1,2,3], PVDM4-64 [1,2,3], PVDM4-128 [1,2,3] and PVDM4-256 [1,2,3]; Firmware Version: IOS-XE 3.13.2
2512	12/24/2015	Christie F-IMB 4K Integrated Media Block (IMB)	Christie Digital Systems Canada, Inc.	Hardware Version: 000-105081-01; Firmware Version: 1.6.0-4217
2513	12/24/2015	Brocade(R) DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones, 6510 FC Switch, 6520 FC Switch, 7800 and 7840 Extension Switch	Brocade Communications Systems, Inc.	Hardware Version: {[DCX Backbone (P/Ns 80-1001064-10, 80-1006751-01, 80-1004920-04 and 80-1006752-01), DCX-4S Backbone (P/Ns 80-1002071-10, 80-1006773-01, 80-1002066-10 and 80-1006772-01), DCX 8510-4 Backbone (P/Ns 80-1004697-04, 80-1006963-01, 80-1005158-04 and 80-1006964-01), DCX 8510-8 Backbone (P/Ns 80-1004917-04 and 80-1007025-01)] with Blades (P/Ns 80-1001070-07, 80-1006794-01, 80-1004897-01, 80-1004898-01, 80-1002000-02, 80-1006771-01, 80-1001071-02, 80-1006750-01, 80-1005166-02, 80-1005187-02, 80-1001066-01, 80-1006936-01, 80-1001067-01, 80-1006779-01, 80-1001453-01, 80-1006823-01, 80-1003887-01, 80-1007000-01, 80-1002839-03, 80-1007017-01, 49-1000016-04, 49-1000064-02 and 49-1000294-05), 6510 FC Switch (P/Ns 80-1005232-03, 80-1005267-03, 80-1005268-03, 80-1005269-03, 80-1005271-03 and 80-1005272-03), 6520 FC Switch (P/Ns 80-1007245-03, 80-1007246-03, 80-1007242-03, 80-1007244-03, 80-1007257-03), 7800 Extension Switch (P/Ns 80-1002607-07, 80-1006977-02, 80-1002608-07, 80-1006980-02, 80-1002609-07 and 80-1006979-02), 7840 (P/N 80-1008000-01)} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v7.3.0 (P/N 63-1001447-01)
2514	12/24/2015	Aruba AP-204 and AP-205 Wireless Access Points	Aruba Networks, Inc.	Hardware Version: AP-204-F1 and AP-205-F1 with FIPS kit 4011570-01; Firmware Version: ArubaOS 6.4.3-FIPS
2515	12/29/2015	FortiManager 5.2	Fortinet, Inc.	Firmware Version: v5.2.4-build0738 150923 (GA)

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2516	12/29/2015	Brocade VDX 6740, VDX 6740T and VDX 8770 Switches	Brocade Communications Systems, Inc.	Hardware Version: {[BR-VDX8770-4-BND-AC (80-1005850-02), BR-VDX8770-4-BND-DC (80-1006532-03), BR-VDX8770-8-BND-AC (80-1005905-02), BR-VDX8770-8-BND-DC (80-1006533-03)] with FRUs (80-1006540-01, 80-1006539-02, 80-1006430-01, 80-1006080-01, 80-1006295-01, 80-1006294-02, 80-1006431-01 and 80-1006429-01), BR-VDX6740-24-F (80-1007295-01), BR-VDX6740-24-R (80-1007294-01), BR-VDX6740-48-F (80-1007483-01), BR-VDX6740-48-R (80-1007481-01), BR-VDX6740-64-ALLSW-F (80-1007484-01), BR-VDX6740-64-ALLSW-R (80-1007482-01), BR-VDX6740T-24-F (80-1007273-01), BR-VDX6740T-24-R (80-1007274-01), BR-VDX6740T-48-F (80-1007485-01), BR-VDX-6740T-48-R (80-1007487-01), BR-VDX6740T-64-ALLSW-F (80-1007486-01), BR-VDX6740T-64-ALLSW-R (80-1007488-01), BR-VDX6740T-56-1G-R (80-1007863-03) and BR-VDX6740T-56-1G-F (80-1007864-03)} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Network OS (NOS) v5.0.0 P/N: 63-1001501-01