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

August 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: Michael J Cooper

Dated: 1 Sep 2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature:

Dated: 1 Sep 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2693	08/03/2016	Forcepoint Sidewinder	Forcepoint	Firmware Version: 8.3.2P07 with patch 8.3.2E106
2694	08/03/2016	Hitachi Virtual Storage Platform (VSP) Encryption Board	Hitachi, Ltd.	Hardware Version: HM800SL1; Firmware Version: 03.07.49.00, 03.07.54.00 or 03.07.56.00
2695	08/03/2016	Seagate Secure® TCG Opal SSC Self-Encrypting Drive (SED) FIPS 140-2 Module	Seagate Technology LLC	Hardware Version: ST1000LM038 - 1RD172 [1], ST2000LM010 - 1RA174 [2]; Firmware Version: SDM1 [1,2], RSE1 [1], LSM1 [1,2], RDE1 [2]
2696	08/04/2016	Juniper Networks SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways	Juniper Networks, Inc.	Hardware Version: P/Ns {SRX100H, SRX100H2, SRX100H-TAA, SRX110H2-VA, SRX110H2-VB, SRX110H-VA, SRX110H-VB; SRX210HE, SRX210HE2, SRX210HE2-POE, SRX210HE-POE, SRX210HE-POE-TAA, SRX210HE-TAA, SRX210H2-POE-TAA, SRX210H2-TAA; SRX220H, SRX220H2, SRX220H-POE, SRX220H2-POE; SRX240H, SRX240H2, SRX240H2-DC, SRX240H2-POE, SRX240H-DC, SRX240H-POE, SRX240H-POE-TAA, SRX240H-TAA, SRX240H2-DC-TAA, SRX240H2-POE-TAA, SRX240H2-TAA; SRX550-645AP, SRX550-645DP, SRX550-645AP-TAA, SRX550-645DP-TAA; SRX650-BASE-SRE6-645AP, SRX650-BASE-SRE6-645DP, SRX650B-SRE6-645AP-TAA} with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS-FIPS 12.1X46-D40
2697	08/04/2016	Ciena 6500 Flex3 WaveLogic 3e OCLD Encryption Module	Ciena Corporation	Hardware Version: 1.0 with PCB P/N NTK539QS-220; Firmware Version: 2.00
2698	08/08/2016	Oracle Solaris Kernel Cryptographic Framework	Oracle Corporation	Software Version: 1.3
2699	08/08/2016	Oracle Solaris Userland Cryptographic Framework	Oracle Corporation	Software Version: 1.3
2700	08/26/2016	Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, Windows 10 for Surface Hub	Microsoft Corporation	Software Version: 10.0.10586
2701	08/26/2016	BitLocker(R) Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, Windows 10 for Surface Hub	Microsoft Corporation	Software Version: 10.0.10586
2702	08/26/2016	BitLocker(R) Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise	Microsoft Corporation	Software Version: 10.0.10586

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
2703	08/26/2016	BitLocker(R) Dump Filter (dumpfve.sys) in Microsoft Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, Windows 10 for Surface Hub	Microsoft Corporation	Software Version: 10.0.10586
2704	08/08/2016	Cisco Catalyst 3750-X Switch	Cisco Systems, Inc.	Hardware Version: WS-C3750X-24T with C3KX-SM-10G, C3KX-NM-1G, C3KX-NM-10G, C3KX-NM-BLANK, or C3KX-NM-10GT; Firmware Version: 15.2(3)E1
2705	08/08/2016	Enhanced Bandwidth Efficient Modem (EBEM) Cryptographic Module	ViaSat, Inc.	Hardware Version: P/Ns 1010162 Version 1, 1010162 with ESEM Version 1, 1091549 Version 1, 1075559 Version 1, 1075559 with ESEM Version 1, 1091551 Version 1, 1010163 Version 1, 1010163 with ESEM Version 1, 1091550 Version 1, 1075560 Version 1, 1075560 with ESEM Version 1 and 1091552 Version 1; P/N 1047117 (tamper evident seal applied over ESEM); Firmware Version: 02.08.13
2706	08/09/2016	V-Key Cryptographic Module	V-Key	Software Version: 3.6.0
2707	08/09/2016	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type B	Toshiba Corporation	Hardware Version: A2 with PX04SVQ040B, PX04SVQ080B, PX04SVQ160B or PX04SRQ192B; Firmware Version: PD09
2709	08/11/2016	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type A	Toshiba Corporation	Hardware Version: A0 with PX04SVQ080B, PX04SVQ160B or PX04SRQ384B; Firmware Version: ZZ01
2710	08/12/2016	Standalone IMB	GDC Technology (USA), LLC	Hardware Version: GDC-IMB-v3, R12; Firmware Version: 2.5 with Security Manager Firmware Version 1.5.0
2711	08/15/2016	Red Hat Enterprise Linux NSS Cryptographic Module v4.0	Red Hat(R), Inc.	Software Version: 4.0
2712	08/16/2016	Imprivata FIPS 140-2 Cryptographic Module	Imprivata	Software Version: 3.6.0 and 3.6.6
2713	08/18/2016	INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit	INTEGRITY Security Services	Firmware Version: 3.0.1
2714	08/19/2016	IDPrime MD 830-revB	Gemalto	Hardware Version: SLE78CFX3000PH; Firmware Version: IDCore30-revB - Build 06, IDPrime MD Applet V4.3.5.D and MSPNP Applet V1.2
2715	08/22/2016	IBM Java JCE FIPS 140-2 Cryptographic Module	IBM Corporation	Software Version: 1.8

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2716	08/22/2016	HGST Ultrastar® SSD800MH.B, SSD1600MM and SSD1600MR TCG Enterprise SSD	HGST, a Western Digital company	Hardware Version: P/Ns HUSMH8080BSS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMH8040BSS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMH8020BSS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMH8010BSS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMM1616ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMM1680ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMM1640ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMM1620ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMR1619ASS235 (0003) [11] HUSMR1619ASS205 (0003) [12, 13] HUSMR1616ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMR1610ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMR1680ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMR1650ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMR1640ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] HUSMR1625ASS205 (0003) [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]; Firmware Version: D326 [1], D327 [2], D370 [3], K326 [4], K370 [5], P326 [6], P33G [7], P344 [8], P370 [9], Q4CB [10], R1C0 [11], G192 [12] or R192 [13]
2717	08/22/2016	FinalCode FIPS Crypto Module for Mobile	FinalCode, Inc.	Software Version: 1.1
2718	08/22/2016	Christie F-IMB 4K Integrated Media Block (IMB)	Christie Digital Systems Canada Inc.	Hardware Version: 000-105081-01; Firmware Version: 1.6.0-4363
2719	08/24/2016	Juniper Networks SRX1400, SRX3400, and SRX3600 Services Gateways	Juniper Networks, Inc.	Hardware Version: P/Ns SRX1400BASE-GE-AC with [1] or [2], SRX1400BASE-GE-DC with [1] or [2], SRX1400BASE-XGE-AC with [1] or [2], SRX1400BASE-XGE-DC with [1] or [2], SRX3400BASE-AC with [2], SRX3400BASE-DC with [2], SRX3400BASE-DC2 with [2], SRX3600BASE-AC with [2], SRX3600BASE-DC with [2], and SRX3600BASE-DC2 with [2]; Service Processing Cards SRX1K-NPC-SPC-1-10-40 [1] or SRX3K-SPC-1-10-40 [2]; with Tamper Seals JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS-FIPS 12.1X46-D40
2720	08/26/2016	Cryptographic Module for Intel(R) vPro(TM) Platforms' Security Engine Chipset	Intel Corporation	Hardware Version: 3.0; Firmware Version: 1.0
2721	08/29/2016	Red Hat Enterprise Linux Libreswan Cryptographic Module v4.0	Red Hat(R), Inc.	Software Version: 4.0
2722	08/26/2016	SPYRUS MDTU-P384 Encryption Module	SPYRUS, Inc.	Hardware Version: P/N 880074014F, Version 2.00.02; Firmware Version: 03.00.0D
2723	08/26/2016	IDCore 30-revB	Gemalto	Hardware Version: SLE78CFX3000PH; Firmware Version: IDCore 30 rev B - Build 06, Demonstration Applet version V1.1
2724	08/29/2016	Cisco Catalyst 3560-CX Switch	Cisco Systems, Inc.	Hardware Version: WS-3560CX-8TC-S; Firmware Version: 15.2(3)E1
2725	08/29/2016	FinalCode FIPS Crypto Module	FinalCode, Inc.	Software Version: 1.1

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
2726	08/29/2016	Xperia Cryptographic Module	Sony Mobile Communications, Inc.	Software Version: 1.0.0
2727	08/29/2016	Hitachi Virtual Storage Platform (VSP) Encryption Adapter	Hitachi, Ltd.	Hardware Version: P/N: eSCAx(WP820) Version: B/A5, B/A6 or B/A7; Firmware Version: 02.09.28.00, 02.09.32.00 or 02.09.37.00
2728	08/29/2016	BlackBerry Linux Kernel Cryptographic Module	BlackBerry Limited	Software Version: 1.0
2729	08/31/2016	Brocade(R) FCX 624/648, ICX 6450, ICX 7750, ICX 7250 and SX 800/1600 Series	Brocade Communications Systems, Inc.	Hardware Version: {[FCX624S (80-1002388-08), FCX624S-HPOE-ADV (80-1002715-08), FCX624S-F-ADV (80-1002727-07), FCX648S (80-1002392-08), FCX648S-HPOE (80-1002391-10), FCX648S-HPOE-ADV (80-1002716-10), FCX-2XG (80-1002399-01)], [ICX6450-24 (80-1005997-03), ICX6450-24P (80-1005996-04), ICX6450-48 (80-1005999-04), ICX6450-48P (80-1005998-04), ICX6450-C12-PD (80-1007578-01)], [ICX7250-24P (80-1008381-02), ICX7250-24G (80-1008379-02), ICX7250-24 (80-1008380-02), ICX7250-48P (80-1008386-02), ICX7250-48 (80-1008384-02)], [ICX7750-48F (80-1007607-01), ICX7750-48C (80-1007608-01), ICX7750-26Q (80-1007609-01), with Components (80-1007871-01; 80-1007870-01; 80-1007738-01; 80-1007737-01; 80-1007761-01; 80-1007760-01; 80-1007632-01)], [FI-SX800-S (80-1003050-03; 80-1007143-03), FI-SX1600-AC (80-1002764-02; 80-1007137-02), with Components (80-1002957-03; 80-1006607-01; 80-1006486-02; 80-1003883-02; 11456-005; 11457-006; 18072-004)]} with FIPS Kit XBR-000195 (80-1002006-02); Firmware Version: IronWare R08.0.30b
2730	08/31/2016	Juniper Networks SRX5400, SRX5600, and SRX5800 Services Gateways	Juniper Networks, Inc.	Hardware Version: P/Ns {SRX5400 (SRX5400B2-AC, SRX5400B2-DC, SRX5400BB-AC, or SRX5400BB-DC), SRX5600 (SRX5600BASE-AC or SRX5600BASE-DC), and SRX5800 (SRX5800BASE-AC or SRX5800BASE-DC)} with Service Processing Cards (SRX5K-SPC-2-10-40 or SRX5K-SPC-4-15-320) and Tamper Seals (JNPR-FIPS-TAMPER-LBLS); Firmware Version: JUNOS-FIPS 12.1X46-D40
2731	08/31/2016	IronKey D300 Series USB Flash Drive	Kingston Technology Company, Inc.	Hardware Version: IKD300 Version 1.0 [4GB, 8GB, 16GB, 32GB, 64GB, 128GB or 256GB]; Firmware Version: 3.05