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

May 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 D Cooper

Dated: 7 June 2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature:

Dated: 6 June 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2629	05/01/2016	ZBR-88W8787-WLAN	Zebra Technologies, Corp.	Hardware Version: P/N: 88W8787, Version 1.0; Firmware Version: Marvell Firmware Version 14.66.35.p51; Zebra Driver Firmware Version 1.2
2630	05/02/2016	Red Hat Enterprise Linux OpenSSH Server Cryptographic Module	Red Hat(R), Inc.	Software Version: 4.0
2631	05/03/2016	Intel OpenSSL FIPS Object Module	Intel Corporation	Software Version: 2.0.5 and 2.0.8
2632	05/12/2016	Dell SonicWALL SM 9800	Dell Software, Inc.	Hardware Version: P/N 101-500380-71, Rev. A; Firmware Version: SonicOS v6.2.1
2633	05/12/2016	Red Hat Enterprise Linux OpenSSH Client Cryptographic Module	Red Hat(R), Inc.	Software Version: 4.0
2634	05/13/2016	Seagate Secure(R) TCG Enterprise SSC 1200.2 SSD Self-Encrypting Drive	Seagate Technology LLC	Hardware Version: ST400FM0293, ST800FM0213, ST1600FM0023 and ST3200FM0043; Firmware Version: 3504
2635	05/13/2016	Ciena 6500 Packet-Optical Platform 4x10G	Ciena® Corporation	Hardware Version: 2.0; Firmware Version: 2.00
2636	05/13/2016	RDL-3000 and eLTE-MT	Redline Communications	Hardware Version: RDL-3000, eLTE-MT; Firmware Version: 3.1
2637	05/13/2016	PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series and PA-7050 Firewalls	Palo Alto Networks	Hardware Version: PA-200 P/N 910-000015-00E Rev. E [1], PA-500 P/N 910-000006-00O Rev. O [2], PA-500-2GB P/N 910-000094-00O Rev. O [2], PA-2020 P/N 910-000004-00Z Rev. Z [3], PA-2050 P/N 910-000003-00Z Rev. Z [3], PA-3020 P/N 910-000017-00J Rev. J [4], PA-3050 P/N 910-000016-00J Rev. J [4], PA-4020 P/N 910-000002-00AB Rev. AB [5], PA-4050 P/N 910-000001-00AB Rev. AB [5], PA-4060 P/N 910-000005-00S Rev. S [5], PA-5020 P/N 910-000010-00F Rev. F [6], PA-5050 P/N 910-000009-00F Rev. F [6], PA-5060 P/N 910-000008-00F Rev. F [6] and PA-7050 P/N 910-000102-00B Rev. B with 910-000028-00B or 910-000117-00A Rev. B [7]; FIPS Kit P/Ns: 920-000084-00A Rev. A [1], 920-000005-00A Rev. A [2], 920-000004-00A Rev. A [3], 920-000081-00A Rev. A [4], 920-000003-00A Rev. A [5], 920-000037-00A Rev. A [6], and 920-000112-00A Rev. A [7]; Firmware Version: 7.0.1-h4 and 7.0.3
2638	05/13/2016	nShield F3 10+, nShield F3 500+, nShield F3 6000+, nShield F3 500+ for nShield Connect+, nShield F3 1500+ for nShield Connect+ and nShield F3 6000+ for nShield Connect+	Thales e-Security Inc.	Hardware Version: nC4033E-010, nC4433E-500, nC4433E-6K0, nC4433E-500N, nC4433E-1K5N and nC4433E-6K0N, Build Standard N; Firmware Version: 2.61.2-2

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
2639	05/13/2016	MiniHSM, MiniHSM for nShield Edge F3, and MiniHSM for Time Stamp Master Clock	Thales e-Security Inc.	Hardware Version: nC4031Z-10, nC4031U-10 and TSMC200, Build Standard N; Firmware Version: 2.61.1-3
2640	05/13/2016	nShield F3 6000e, nShield F3 1500e, nShield F3 500e, nShield F3 10e, nShield F3 6000e for nShield Connect, nShield F3 1500e for nShield Connect and nShield F3 500e for nShield Connect	Thales e-Security Inc.	Hardware Version: nC4033E-6K0, nC4033E-1K5, nC4033E-500, nC4033E-010, nC4033E-6K0N, nC4033E-1K5N and nC4033E-500N, Build Standard N; Firmware Version: 2.61.2-3
2641	05/13/2016	nShield F2 6000e, nShield F2 1500e, nShield F2 500e and nShield F2 10e	Thales e-Security Inc.	Hardware Version: nC3023E-6K0, nC3023E-1K5, nC3023E-500 and nC3023E-010, Build Standard N; Firmware Version: 2.61.2-2
2642	05/13/2016	MiniHSM, MiniHSM for nShield Edge F2, and MiniHSM for Time Stamp Master Clock	Thales e-Security Inc.	Hardware Version: nC4031Z-10, nC3021U-10, and TSMC200, Build Standard N; Firmware Version: 2.61.1-2
2643	05/13/2016	nShield F2 500+, nShield F2 1500+ and nShield F2 6000+	Thales e-Security Inc.	Hardware Version: nC3423E-500, nC3423E-1K5 and nC3423E-6K0, Build Standard N; Firmware Version: 2.61.2-2
2644	05/13/2016	nShield F3 10+, nShield F3 500+, nShield F3 6000+, nShield F3 500+ for nShield Connect+, nShield F3 1500+ for nShield Connect+ and nShield F3 6000+ for nShield Connect+	Thales e-Security Inc.	Hardware Version: nC4033E-010, nC4433E-500, nC4433E-6K0, nC4433E-500N, nC4433E-1K5N and nC4433E-6K0N, Build Standard N; Firmware Version: 2.61.2-3
2645	05/13/2016	RF-7800W Broadband Ethernet Radio	Harris Corporation	Hardware Version: RF-7800W-OU50x, OU47x and OU49x; Firmware Version: 4.10
2646	05/13/2016	Samsung Flash Memory Protector V1.1	Samsung Electronics Co., Ltd.	Software Version: 1.2; Hardware Version: 3.0.1
2647	05/25/2016	SPYCOS® 3.0 QFN	SPYRUS, Inc.	Hardware Version: 742100004F; Firmware Version: 3.0.2
2648	05/27/2016	NetApp Cryptographic Security Module	NetApp, Inc.	Software Version: 1.0

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
2649	05/27/2016	Brocade(R) ICX (TM) 6610 and ICX 7450 Series	Brocade Communications Systems, Inc.	Hardware Version: {ICX6610-24F-I (80-1005350-04), ICX6610-24F-E (80-1005345-04), ICX6610-24-I (80-1005348-05), ICX6610-24-E (80-1005343-05), ICX6610-24P-I (80-1005349-06), ICX6610-24P-E (80-1005344-06), ICX6610-48-I (80-1005351-05), ICX6610-48-E (80-1005346-05), ICX6610-48P-I (80-1005352-06), ICX6610-48P-E (80-1005347-06), ICX7450-24 (80-1008060-01), ICX7450-24P (80-1008061-01), ICX7450-48 (80-1008062-01), ICX7450-48P (80-1008063-01), ICX7450-48F (80-1008064-01), with Components (80-1005261-04; 80-1005259-04; 80-1005262-03; 80-1005260-03; 80-1007165-03; 80-1007166-03; 80-1008334-01; 80-1008333-01; 80-1008332-01; 80-1008331-01; 80-1008308-01; 80-1008309-01; 123400000829A-R01; 123400000830A-R01; 123400000833A-R01)} with FIPS Kit XBR-000195 (80-1002006-02); Firmware Version: IronWare R08.0.30b