

FIPS 140-2 Consolidated Validation Certificate



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



September 2018



The Communications Security Establishment of the
Government of Canada

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: 10/3/2018
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature: [Signature]
Dated: 2018-10-02
A/ Director, Security Architecture and Risk Management
Communications Security Establishment

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3194	09/26/2018	Windows OS Loader	Microsoft Corporation	Software Version: 10.0.15063.674 [1], 10.0.15254 [2] and 10.0.16299 [3]
3196	09/26/2018	Kernel Mode Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.15063.674 [1], 10.0.15254 [2] and 10.0.16299 [3]
3277	09/04/2018	FastIron ICX™ 7750, ICX™ 7250 and ICX™ 7150 Series Switch/Router	Ruckus Wireless, Inc.	Hardware Version: Base Models: ICX7150-C12P-2X10GR-A [1], ICX7150-24-4X10GR-A [2], ICX7150-24P-4X10GR-A [3], ICX7150-48-4X10GR-A [4], ICX7150-48P-4X10GR-A [5], ICX7150-48PF-4X10GR-A [6], ICX7150-48ZP-8X10GR2-A [7], ICX7250-24G [8], ICX7250-48P [9], ICX7750-48F [10], ICX7750-48C [11], ICX7750-26Q [12]; with Power Supply components: RPS20 [7], EPS4000 [8, 9], RPS17 [7, 8, 9], RPS9I [10, 11, 12], RPS9E [10, 11, 12], RPS9DCI [10, 11, 12], RPS9DCE [10, 11, 12]; with Fan components: ICX-FAN11 [7], ICX7750-FAN-I [10, 11, 12], ICX7750-FAN-E [10, 11, 12], ICX7750-FAN-I SINGLE [10, 11, 12], ICX7750-FAN-E SINGLE [10, 11, 12]; and optional component: ICX7750-6Q [10, 11, 12]; Firmware Version: IronWare R08.0.70
3278	09/04/2018	Hitachi Virtual Storage Platform (VSP) Encryption Module	Hitachi, Ltd.	Hardware Version: P/N: 3289094-A(BS12GE) Version: B/D4, B/D5, B/D4a, B/D5a, B/D6, B/D7 or B/D8; Firmware Version: 03.09.34.00
3279	09/04/2018	Hitachi Virtual Storage Platform (VSP) Encryption Board	Hitachi, Ltd.	Hardware Version: HM800SL1 or HM800SL1a; Firmware Version: 03.09.34.00
3280	09/05/2018	NITROX XL 1600-NFBE HSM Family	Cavium Inc.	Hardware Version: 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 and CN16XX-NFBE-FW-2.3-180821
3281	09/05/2018	Mojo Wireless Manager	Mojo Networks, Inc.	Firmware Version: MA-VM 8.2.1
3282	09/12/2018	HPE LTO-7 Encrypting Tape Drive	Hewlett Packard Enterprise	Hardware Version: AQ308A#103 [1], AQ303A#103 [2]; Firmware Version: LTO_15000_FC_G986_MSL_S.frm [1], LTO_15000_SAS_G986_MSL_S.frm [2]
3284	09/12/2018	Cryptographic Module for Fognigma	Berryville Holdings, LLC	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
3285	09/13/2018	Unisys OS 2200 Cryptographic Library	Unisys Corporation	Software Version: 2R1
3286	09/17/2018	Cisco Adaptive Security Appliances Cryptographic Module	Cisco Systems, Inc.	Hardware Version: [ASA 5506-X, ASA 5506H-X, ASA 5506W-X] with [1][2], ASA 5508-X with [1][3], ASA 5516-X with [1][4], and [ASA 5525-X, ASA 5545-X, ASA 5555-X] with [1]; FIPS Kit: [AIR-AP-FIPSKIT=][1], [ASA5506-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3] or [ASA5516-FIPS-KIT=][4]; Firmware Version: 9.8
3287	09/18/2018	Cisco Firepower Threat Defense on 4K/9K 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: 6.2
3288	09/19/2018	Juniper Networks NFX250 Network Services Platform	Juniper Networks, Inc.	Hardware Version: NFX250-S1, NFX250-S2; Firmware Version: Junos OS 17.3R2

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3289	09/20/2018	SonicWALL TZ 300/TZ 300W, TZ 400/TZ 400W, TZ 500/TZ 500W, TZ 600, SOHOW, SM 9200, SM 9400, SM 9600 and NS _a 2650, NS _a 3600, NS _a 3650, NS _a 4600, NS _a 4650, NS _a 5600, NS _a 5650, NS _a 6600	SonicWall, Inc.	Hardware Version: 101-500410-54 Rev. E (SOHOW), 101-500403-55 Rev. F (TZ 300), 101-500404-54 Rev. E (TZ 300W), 101-500405-55 Rev. F (TZ 400), 101-500406-54 Rev. E (TZ 400W), 101-500411-56 Rev. G (TZ 500), 101-500412-55 Rev. F (TZ 500W), 101-500413-56 Rev. G (TZ 600), 101-500452-50 Rev. A (NS _a 2650), 101-500459-54 Rev. E (NS _a 3600), 101-500514-50, (NS _a 3650), 101-500458-54 Rev. E (NS _a 4600), 101-500451-50 (NS _a 4650), 101-500457-54 Rev. E (NS _a 5600), 101-500517-50 (NS _a 5650), 101-500456-54 Rev. E (NS _a 6600), 101-500455-54 Rev. E (SM 9200), 101-500454-54 Rev. E (SM 9400), 101-500453-54 Rev. E (SM 9600); Firmware Version: SonicOS v6.5.1
3290	09/21/2018	TMC TCG Enterprise SSC Crypto Sub-Chip	Toshiba Memory Corporation	Hardware Version: 0000; Firmware Version: SC01
3291	09/25/2018	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.9
3292	09/25/2018	Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: 6.0
3293	09/25/2018	Red Hat Enterprise Linux Libreswan Cryptographic Module	Red Hat(R), Inc.	Software Version: 6.0
3294	09/26/2018	iStorage FIPS 140-2 Level 2 Module Rev 1.0	iStorage Ltd.	Hardware Version: Rev 1.0; Firmware Version: EC Firmware version IS_EC_FW_2_59_1X and SC Firmware version 1.6
3295	09/26/2018	iStorage diskAshur PRO ² Level 2 Secure Storage Drive	iStorage Ltd.	Hardware Version: IS-DAP2-256-500-C-X, IS-DAP2-256-1000-C-X, IS-DAP2-256-2000-C-X, IS-DAP2-256-3000-C-X, IS-DAP2-256-4000-C-X, IS-DAP2-256-5000-C-X, IS-DAP2-256-SSD-128-C-X, IS-DAP2-256-SSD-256-C-X, IS-DAP2-256-SSD-512-C-X, IS-DAP2-256-SSD-1000-C-X, IS-DAP2-256-SSD-2000-C-X, IS-DAP2-256-SSD-4000-C-X; Firmware Version: EC Firmware version IS_EC_FW_2_59_1X and SC Firmware version 1.6
3296	09/26/2018	FastIron ICX™ 7650 Series Switch/Router	Ruckus Wireless, Inc.	Hardware Version: P/Ns ICX7650-48F, ICX7650-48P and ICX7650-48ZP; Firmware Version: IronWare R08.0.70
3297	09/27/2018	SecureDrive KP	SECUREDATA, Inc.	Hardware Version: SD-KP-12-BL-1TB, SD-KP-12-BL-2TB, SD-KP-20-BL-1TB, SD-KP-20-BL-2TB, SD-KP-20-BL-4TB, SD-KP-20-BL-5TB; Firmware Version: CLEVX_3637E_USB_V0313 and CLEVX_SATA-KP_v2.2