FIPS 140-2 Consolidated Validation Certificate

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

The Canadian Centre for Cyber Security

August 2020

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, 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: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: September 3, 2020

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3695	08/06/2020	Cisco Firepower Threat Defense Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR1010[1], FPR1120[2], FPR1140[2], FPR2110[3], FPR2120[3], FPR2130[3] and FPR2140[3] with FIPS Kit (AIR-AP-FIPSKIT=) and Opacity Shield 800-44098-01[1], 800-45098-01[2] and 69-100250-01[3]; Firmware Version: 6.4
3696	08/12/2020	Ruckus Wireless Cloudpath Enrollment System	Ruckus Wireless, Inc.	Software Version: 5.3
3697	08/17/2020	Ultrastar® DC HC530 TCG Enterprise HDD	Western Digital Corporation	Hardware Version: P/Ns WUH721414AL5205 and WUH721414AL4205; Firmware Version: R221, R240 or 3P00
3698	08/17/2020	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 R08.0.90a
3699	08/17/2020	Oracle Linux 7 Libreswan Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
3700	08/17/2020	FastIron ICX™ 7450 Series Switch/Router	Ruckus Wireless, Inc.	Hardware Version: ICX7450-24P, ICX7450-48P, ICX7450-48F, ICX7400-4X1GF, ICX7400-4X10GF, ICX7400-4X10GC, ICX7400-1X40GQ, ICX7400-SERVICE-MOD, RPS16-E, RPS16DC-E, RPS16-I, RPS16DC-I, ICX-FAN10-I, ICX-FAN10-E, Filler Panel; Firmware Version: IronWare R08.0.90a
3701	08/17/2020	FastIron ICX™ 7650 Series Switch/Router	Ruckus Wireless, Inc.	Hardware Version: P/Ns ICX7650-48F, ICX7650-48P and ICX7650-48ZP; Firmware Version: IronWare R08.0.90a
3702	08/19/2020	D2iQ BoringCrypto Cryptographic Security Module	D2iQ Inc.	Software Version: 66005f41fbc3529ffe8d007708756720529da20d
3703	08/24/2020	Aegis Secure Key 3NX Cryptographic Module	Apricorn	Hardware Version: P/Ns ASK3NX-2GB, ASK3NX-4GB, ASK3NX-8GB, ASK3NX-16GB, ASK3NX-32GB, ASK3NX-64GB, ASK3NX-128GB; Hardware Version: Rev A1; Firmware Version: 1.5
3704	08/29/2020	Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access points, Version 8.10, 16.12	Cisco Systems, Inc.	Hardware Version: 1562e, 1562i, 1562d, 1562ps, 2802e, 2802i, 3802e, 3802i, 3802p and 4800 with FIPS Kit: AIR-AP-FIPSKIT=; Firmware Version: 8.10, 16.12