FIPS 140-2 Consolidated Validation Certificate
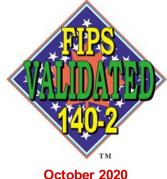

The National Institute of Standards and Technology of
the United States of America

October 2020

The Canadian Centre for Cyber Security

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: _____*Gavin O'Brien*_____

Dated: _____December 7, 2020_____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____November 24, 2020_____

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3719	10/02/2020	OpenSSH Client Cryptographic Module for Perimeta SBC	Metaswitch Networks Ltd	Software Version: 1.0
3720	10/02/2020	OpenSSH Server Cryptographic Module for Perimeta SBC	Metaswitch Networks Ltd	Software Version: 1.0
3721	10/02/2020	Samsung NVMe TCG Opal SSC SEDs PM1723b Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLL3T8HAJQ-000G6, MZWLL3T8HAJQ-00AG6 and MZWLL15THMLA-00AG6; Firmware Version: NA04
3722	10/06/2020	FibeAir® IP-20C, FibeAir® IP-20C-HP, FibeAir® IP-20C 2E2SX, FibeAir® IP-20S, FibeAir® IP-20N, FibeAir® IP-20A, FibeAir® IP-20G, and FibeAir® IP-20GX	Ceragon Networks, Ltd.	Hardware Version: [IP-20N and IP-20A with components IP-20-TCC-B-MC+SD-AF: 24-T009-1|A, IP-20-TCC-B-MC+SD-AF: 24-T009-1|B, IP-20-TCC-B-MC+SD-AF: 24-T009-1|C, IP-20-TCC-B2+SD-AF: 24-T010-1|A, IP-20-TCC-B2+SD-AF: 24-T010-1|B, IP-20-TCC-B2-XG-MC+SD-AF: 24-T011-1|A, IP-20-TCC-B2-XG-MC+SD-AF: 24-T011-1|B, IP-20-TCC-B2-XG-MC+SD-AF: 24-T011-1|C, IP-20-RMC-B-AF: 24-R010-0|A, IP-20-RMC-B-AF: 24-R010-1|A, and IP-20-RMC-B-AF: 24-R010-1|B], [IP-20GX with components IP-20-RMC-B-AF: 24-R010-0|A, IP-20-RMC-B-AF: 24-R010-1|A, and IP-20-RMC-B-AF: 24-R010-1|B], [IP-20C], [IP-20C-HP], [IP-20C 2E2SX], [IP-20S], [IP-20G]; Firmware Version: CeraOS 10.9.6b74
3723	10/06/2020	Cisco Systems 3504, 5520, and 8540 Wireless LAN Controllers, Version 8.10	Cisco Systems, Inc.	Hardware Version: 3504, 5520 and 8540; Firmware Version: 8.10
3724	10/07/2020	Ubuntu 16.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3725	10/09/2020	Ubuntu 16.04 OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3726	10/19/2020	nShield F2 500+ & nShield F2 1500+ & nShield F2 6000+	nCipher Security Limited	Hardware Version: nC3423E-500, nC3423E-1K5 and nC3423E-6K0, Build Standard N; Firmware Version: 12.50.8
3727	10/20/2020	MiniHSM, MiniHSM for nShield Edge F3, and MiniHSM for Time Stamp Master Clock	nCipher Security Limited	Hardware Version: nC4031Z-10, nC4031U-10 and TSMC200, Build Standard N; Firmware Version: 12.50.8
3728	10/20/2020	Cisco Firepower Management Center Virtual (FMCv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.4
3729	10/21/2020	Symantec PGP Cryptographic Engine	Symantec Corporation	Software Version: 4.4
3730	10/21/2020	nShield F3 10+ 500+ 6000+ & nShield F3 500+ 1500+ 6000+ for nShield Connect+	nCipher Security Limited	Hardware Version: nC4033E-010, nC4433E-500, nC4433E-6K0, nC4433E-500N, nC4433E-1K5N and nC4433E-6K0N, Build Standard N; Firmware Version: 12.50.8

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3731	10/21/2020	nShield F3 10+ 500+ 6000+ & nShield F3 500+ 1500+ 6000+ for nShield Connect+	nCipher Security Limited	Hardware Version: nC4033E-010, nC4433E-500, nC4433E-6K0, nC4433E-500N, nC4433E-1K5N and nC4433E-6K0N, Build Standard N; Firmware Version: 12.50.8
3732	10/22/2020	Citrix ADC VPX	Citrix Systems, Inc.	Software Version: 12.1.51.152
3733	10/23/2020	Fornetix® Key Orchestration(tm)	Fornetix LLC	Hardware Version: KO-2000; Firmware Version: 2.2-FIPS
3734	10/27/2020	Aruba Virtual and Hardware Mobility Master Appliances with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Firmware Version: ArubaOS 8.2.2.5-FIPS, ArubaOS 8.5.0.3-FIPS and ArubaOS 8.6.0.4-FIPS
3735	10/27/2020	Aruba Mobility Controller Virtual Appliances with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Firmware Version: ArubaOS 8.2.2.5-FIPS, ArubaOS 8.5.0.3-FIPS and ArubaOS 8.6.0.4-FIPS
3736	10/27/2020	LoadMaster FIPS Object Module	Kemp Technologies Inc.	Software Version: v1.0
3737	10/27/2020	Juniper Networks SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX5400, SRX5600 and SRX5800 Services Gateways	Juniper Networks, Inc	Hardware Version: [SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550, SRX5400, SRX5600 and SRX5800] with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS OS 19.2R1
3738	10/27/2020	Ruckus Wireless, Inc. R710, R610, R720, T610 and T710 Wireless Access Points	Ruckus Wireless, Inc.	Hardware Version: R710, R610, R720, T610 and T710; Firmware Version: 3.6.0.3
3739	10/29/2020	AWS Nitro Card Security Engine	Amazon Web Services, Inc.	Hardware Version: AL5+; Firmware Version: HAL-rel-3.2-uemu-fips
3740	10/29/2020	Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.4
3741	10/30/2020	NITROXIII CNN35XX-NFBE HSM Family	Marvell Semiconductor, Inc.	Hardware Version: P/Ns CNL3560P-NFBE-G [1], CNL3560-NFBE-G [1], CNL3530-NFBE-G [1], CNL3510-NFBE-G [1], CNL3510P-NFBE-G [1], CNN3560P-NFBE-G [1], CNN3560-NFBE-G [1], CNN3530-NFBE-G [1], CNN3510-NFBE-G [1], CNL3560P-NFBE-2.0-G [2], CNL3560-NFBE-2.0-G [2], CNL3530-NFBE-2.0-G [2], CNL3510-NFBE-2.0-G [2], CNL3510P-NFBE-2.0-G [2], CNL3560PB-NFBE-2.0-G [2], CNL3560B-NFBE-2.0-G [2], CNL3530B-NFBE-2.0-G [2], CNL3510B-NFBE-2.0-G [2], CNL3510PB-NFBE-2.0-G [2], CNN3510LP-NFBE-2.0-G [2] and CNN3510LPB-NFBE-2.0-G [2]; Firmware Version: CNN35XX-NFBE-FW-2.04 build 48 [1, 2], CNN35XX-NFBE-FW-2.04 build 49 [1, 2], CNN35XX-NFBE-FW-2.04 build 50 [1, 2], CNN35XX-NFBE-FW-2.04 build 52 [1, 2], CNN35XX-NFBE-FW-2.04 build 53 [1, 2], CNN35XX-NFBE-FW-2.05 build 15 [1] and CNN35XX-NFBE-FW-2.05 build 18 [1]