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

July 2021

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: TIMOTHY HALL Digitally signed by TIMOTHY HALL Date: 2021.08.09 10:17:54 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Sproule, Lisa Digitally signed by Sproule, Lisa DN: C=CA, O=GC, OU=CSE-CST, CN="Sproule, Lisa" Reason: I am the author of this document Location: your signing location here Date: 2021.08.03 13:57:31-04'00' Foxit PhantomPDF Version: 10.1.4

Dated: _____

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
3964	07/01/2021	Motorola Network Router (MNR) S6000	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1780N Rev AB with Encryption Module P/N CLN8261D Rev NB; Firmware Version: 18.2.2.03
3965	07/05/2021	KIOXIA TCG Enterprise SSC Crypto Sub-Chip TC58NC1132GTC	KIOXIA Corporation	Hardware Version: 0001; Firmware Version: SC01AS
3966	07/06/2021	Ubuntu 20.04 OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 3.0
3967	07/06/2021	Extreme Networks SLX 9640, SLX 9150 and SLX 9250 Switches	Extreme Networks, Inc.	Hardware Version: P/Ns EN-SLX- 9640-24S-12C-AC-F, EN-SLX- 9640-24S-12C-AC-R, SLX 9150-48Y-8C-AC-F, SLX 9150-48Y-8C-AC-R, SLX 9150-48XT-6C-AC-F, SLX 9150-48XT-6C-AC-R, SLX 9250-32C-AC-F and SLX 9250-32C-AC-R; Firmware Version: SLXOS 20.1.1aa
3968	07/06/2021	Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE-S-X6-64G Routing Engine and Multiservices MPC	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960 with components identified in Security Policy Table 1; Firmware Version: Junos OS 19.1R2
3969	07/06/2021	Motorola GGM 8000 Gateway	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1841F Rev AG with FIPS Kit P/N CLN8787A Rev B and Power Supply P/N CLN1850A Rev GB (AC) or P/N CLN1849C Rev AB (DC); Firmware Version: 18.2.2.03
3970	07/06/2021	Integral AES 256 Bit Crypto SSD Underlying PCB	Integral Memory Plc	Hardware Version: INSSD128GS625C140, INSSD256GS625C140, INSSD512GS625C140, INSSD1TS625C140, INSSD2TS625C140, INSSD4TS625C140, INSSD128GM280C140, INSSD256GM280C140, INSSD512GM280C140, INSSD1TM280C140, INSSD2TM280C140, INSSD4TM280C140, INSSD128GM280NC140, INSSD256GM280NC140, INSSD512GM280NC140, INSSD1TM280NC140, INSSD2TM280NC140, INSSD4TM280NC140; Firmware Version: SCPJ13.0
3971	07/06/2021	Unisys Linux strongSwan Cryptographic Module	Unisys Corporation	Software Version: 5.6.3-6.4
3972	07/07/2021	DL4FE	DataLocker Inc.	Hardware Version: DL4-500GB-FE, DL4-1TB-FE, DL4-2TB-FE, DL4-SSD-500GB-FE, DL4-SSD-1TB-FE, DL4-SSD-2TB-FE, DL4-SSD-4TB-FE, DL4-SSD-7.6TB-FE, DL4-SSD-16TB-FE; Firmware Version: Firmware Version 1.49 and Bootloader Version 1.12
3973	07/07/2021	VMware's SD-WAN VPN Hybrid Crypto Module	VMware, Inc.	Software Version: 1.0; Hardware Version: Intel Atom C3308, Intel Atom C3558, Intel Atom C3958 and Intel Xeon D-2187NT
3974	07/07/2021	Poly Crypto Module	Plantronics, Inc	Software Version: 2.2
3975	07/12/2021	VMware's SD-WAN VPN Crypto Module	VMware, Inc.	Software Version: 1.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3976	07/12/2021	Keeper Security Cryptographic Module	Keeper Security Inc.	Software Version: 1.0.2.1
3977	07/12/2021	Pavilion Cryptographic Module	Pavilion Data Systems	Software Version: 1.0; Hardware Version: Intel Xeon D-1548
3978	07/12/2021	Corelight Cryptographic Module	Corelight Inc.	Software Version: 2.2
3979	07/12/2021	FEITIAN Biometric FIDO Key Module	FEITIAN Technologies Co., Ltd.	Hardware Version: Z32HUB; Firmware Version: 1.0.03
3980	07/12/2021	Ubuntu 18.04 OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 2.1
3981	07/15/2021	Entrust Authority™ Security Kernel	Entrust Corporation	Software Version: 1.0 and 1.1
3982	07/15/2021	R610-F Access Point, R710 Access Point, R720 Access Point, T610 Access Point, T610s Access Point, T710 Access Point, T710s Access Point, E510 Access Point	Ruckus Wireless, Inc.	Hardware Version: P/Ns 9F1-R610-US00, rev A; 9F1-R710-US00, rev A; 9F1-R720-US00, rev A; 9F1-T610-US01, rev B4; 9F1-T610-US51, rev A; 9F1-T710-US01, rev A; 9F1-T710-US51, rev A; 9F1-E510-US01, rev A; XBR-000195 (Tamper-Evident Seal); Firmware Version: 5.1.1.3
3983	07/15/2021	KIOXIA TCG OPAL SSC Crypto Sub-Chip TC58NC1132GTC	KIOXIA Corporation	Hardware Version: 0001; Firmware Version: SC01AN
3984	07/16/2021	OFSM (Obsidian FIPS Security Module)	Coolrock Software Pty Ltd	Software Version: 1.0.2.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3985	07/16/2021	NITROXIII CNN35XX-NFBE HSM Family	Marvell	Hardware Version: P/Ns CNL3560P-NFBE-G, CNL3560-NFBE-G, CNL3530-NFBE-G, CNL3510-NFBE-G, CNL3510P-NFBE-G, CNN3560P-NFBE-G, CNN3560-NFBE-G, CNN3530-NFBE-G and CNN3510-NFBE-G, Version HW-1.0; CNL3560P-NFBE-2.0-G, CNL3560-NFBE-2.0-G, CNL3530-NFBE-2.0-G, CNL3510-NFBE-2.0-G, CNL3510P-NFBE-2.0-G, CNL3560PB-NFBE-2.0-G, CNL3560B-NFBE-2.0-G, CNL3530B-NFBE-2.0-G, CNL3510B-NFBE-2.0-G, CNL3510PB-NFBE-2.0-G, CNN3510LP-NFBE-2.0-G, CNN3510LPB-NFBE-2.0-G, CNN3560P-NFBE-2.0-G, CNN3560-NFBE-2.0-G, CNN3530-NFBE-2.0-G, CNN3510-NFBE-2.0-G and CNN3505LP-NFBE-2.0-G, Version HW-2.0; CNL3560P-NFBE-3.0-G, CNL3560B-NFBE-3.0-G, CNL3560-NFBE-3.0-G, CNL3560A-NFBE-3.0-G, CNL3560C-NFBE-3.0-G, CNL3560D-NFBE-3.0-G, CNL3560E-NFBE-3.0-G, CNL3560F-NFBE-3.0-G, CNL3560I-NFBE-3.0-G , CNL3530-NFBE-3.0-G, CNL3530B-NFBE-3.0-G, CNL3530A-NFBE-3.0-G, CNL3530C-NFBE-3.0-G, CNL3530D-NFBE-3.0-G, CNL3530E-NFBE-3.0-G, CNL3530F-NFBE-3.0-G, CNL3530I-NFBE-3.0-G , CNL3510-NFBE-3.0-G, CNL3510P-NFBE-3.0-G, CNL3510A-NFBE-3.0-G, CNL3510C-NFBE-3.0-G, CNL3510D-NFBE-3.0-G, CNL3510E-NFBE-3.0-G, CNL3510F-NFBE-3.0-G, CNL3510I-NFBE-3.0-G, CNN3560P-NFBE-3.0-G, CNN3560-NFBE-3.0-G, CNN3560A-NFBE-3.0-G, CNN3560C-NFBE-3.0-G, CNN3560D-NFBE-3.0-G, CNN3560E-NFBE-3.0-G, CNN3560F-NFBE-3.0-G, CNN3530-NFBE-3.0-G, CNN3530A-NFBE-3.0-G, CNN3530C-NFBE-3.0-G, CNN3530D-NFBE-3.0-G, CNN3530E-NFBE-3.0-G, CNN3530F-NFBE-3.0-G, CNN3510-NFBE-3.0-G, CNN3510A-NFBE-3.0-G, CNN3510C-NFBE-3.0-G, CNN3510D-NFBE-3.0-G, CNN3510E-NFBE-3.0-G, CNN3510F-NFBE-3.0-G, CNN3510LP-NFBE-3.0-G, CNN3510LPB-NFBE-3.0-G, CNN3510LPA-NFBE-3.0-G, CNN3510LPC-NFBE-3.0-G, CNN3510LPD-NFBE-3.0-G, CNN3510LPE-NFBE-3.0-G, CNN3510LPF-NFBE-3.0-G, CNN3505LP-NFBE-3.0-G, CNN3505LPA-NFBE-3.0-G, CNN3505LPC-NFBE-3.0-G, CNN3505LPD-NFBE-3.0-G, CNN3505LPE-NFBE-3.0-G, and CNN3505LPF-NFBE-3.0-G, Version HW-3.0; Firmware Version: CNN35XX-NFBE-FW-2.06 build 05, CNN35XX-NFBE-FW-2.06 build 06, CNN35XX-NFBE-FW-2.06 build 07 and CNN35XX-NFBE-FW-2.06 build 08
3986	07/18/2021	mTera 8-slot Universal Transport Platform	Infinera Corporation	Hardware Version: 81.71S-MTERA8-R6 with tamper-evident labels MKS-MSECTAPE-00; Firmware Version: FP5.1.2
3987	07/19/2021	CipherTrust Transparent Encryption Cryptographic Module	Thales	Software Version: 2.0; Hardware Version: 5118 and EPXH
3988	07/19/2021	Cisco ASR 1000 Series Routers without MACSEC	Cisco Systems, Inc.	Hardware Version: ASR1002-X, [ASR1004 and ASR1006 with components ASR-1000-RP2, ASR1000-ESP20 and ASR1000-ESP40]; Firmware Version: IOS-XE 16.9

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3989	07/19/2021	Quadient Postal Security Device (PSD)	Quadient Technologies France	Hardware Version: A0014227-B and A0014227-C; Firmware Version: a30.08 (P/N: A0134483A)
3990	07/20/2021	i.MX 8X SECO HSM	NXP Semiconductors	Hardware Version: P/N: rpp_cm0p_sec_subsys; version tag DA_SSL_iMX8QX_SCU_SUBSYS_LN28FDSOI_1.72.; Firmware Version: ROM mem_i.MX8QX_s28roml_w20480x032m32B2_1Tlms_m0_1.3; SECO FW 3.7.1
3991	07/22/2021	SUSE Linux Enterprise Server OpenSSL Cryptographic Module	SUSE, LLC	Software Version: 4.1
3992	07/22/2021	SUSE Linux Enterprise Server libgcrypt Cryptographic Module	SUSE, LLC	Software Version: 3.1
3993	07/22/2021	Mirantis Cryptographic Module NG	Mirantis, Inc.	Software Version: 2.2
3994	07/27/2021	CommVault Crypto Library	CommVault Systems, Inc.	Software Version: 2.0
3996	07/29/2021	Aegis Fortress L3 Cryptographic Module	Apricorn	Hardware Version: P/Ns AFL3-500, AFL3-1TB, AFL3-2TB, AFL3-3TB, AFL3-4TB, AFL3-5TB, AFL3-S500, AFL3-S1TB, AFL3-S2TB, AFL3-S4TB, AFL3-S8TB, AFL3-S16TB and AFL3-S20TB; Hardware Version: Rev B1; Firmware Version: 3.2