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

January 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: Gavin O'Brien

Dated: 02/19/2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 2021-02-09

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
3788	01/05/2021	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, CNN3510-NFBE-G, Version HW-1.0 and 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 and CNN3510LPB-NFBE-2.0-G, Version HW-2.0; Firmware Version: CNN35XX-NFBE-FW-2.06 build 05 and CNN35XX-NFBE-FW-2.06 build 06
3789	01/06/2021	Cisco ASA Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR4110-ASA-K9, FPR4115-ASA-K9, FPR4120-ASA-K9, FPR4125-ASA-K9, FPR4140-ASA-K9, FPR4145-ASA-K9, FPR4150-ASA-K9, FPR9K-SM-24, FPR9K-SM-36, FPR9K-SM-40, FPR9K-SM-44, FPR9K-SM-48 and FPR9K-SM-56; Firmware Version: 9.12
3790	01/06/2021	Cisco FIPS Object Module	Cisco Systems, Inc.	Firmware Version: 7.2
3791	01/11/2021	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.5
3792	01/13/2021	NRevenector 2018	FP InovoLabs GmbH	Hardware Version: 58.0036.0301.00 and 58.0036.0302.00; Firmware Version: Bootloader 90.0036.0401.00/2019141001
3793	01/20/2021	iStorage datAshur PROÂ² Level 3 Secure Storage Drive	iStorage Ltd.	Hardware Version: IS-FL-DP2-256-4, IS-FL-DP2-256-8, IS-FL-DP2-256-16, IS-FL-DP2-256-32, IS-FL-DP2-256-64, IS-FL-DP2-256-128, IS-FL-DP2-256-256, and IS-FL-DP2-256-512; Firmware Version: EC Firmware version IS_EC_FW_505_1X and SC Firmware version 2.5
3794	01/21/2021	Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20190926
3795	01/21/2021	Cisco Firepower 4100 and Cisco Firepower 9300 Series	Cisco Systems, Inc.	Hardware Version: FPR4110-NGFW-K9[1], FPR4115-NGFW-K9[1], FPR4120-NGFW-K9[1], FPR4125-NGFW-K9[1], FPR4140-NGFW-K9[1], FPR4145-NGFW-K9[1], FPR4150-NGFW-K9[1], FPR9K-Sup (SM-24)[2], FPR9K-Sup (SM-36)[2], FPR9K-Sup (SM-40)[2], FPR9K-Sup (SM-44)[2], FPR9K-Sup (SM-48)[2] and FPR9K-Sup (SM-56)[2] with FIPS Kit (Cisco_TEL.FIPS_Kit), and opacity shield 69-100250-01[1] or 800-102843-01[2]; Firmware Version: 2.6
3796	01/25/2021	IDPrime 930 / 3930	Thales	Hardware Version: SLE78CFX400VPH - A1977038, SLE78CLFX400VPH - A1714221, SLE78CFX400VPH - A2023188 and SLE78CFX400VPH - A2410334; Firmware Version: IDCore3130 - Build 11D, IDPrime 930/3930 Applet V4.5 and MSPNP Applet V1.2
3797	01/25/2021	SUSE Linux Enterprise Server OpenSSL Cryptographic Module	SUSE, LLC	Software Version: 4.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3798	01/25/2021	Network Security Platform Sensor NS3500	McAfee, LLC	Hardware Version: P/Ns IPS-NS3500 Version 1.10; Firmware Version: 10.1.17.1
3799	01/26/2021	ePass2003 Cryptographic Module	Feitian Technologies Co., Ltd.	Hardware Version: ePass2003-A3 and ePass2003-X15; Firmware Version: 1.0.11
3800	01/26/2021	VNX 6 Gb/s SAS I/O Module with Encryption	Dell EMC	Hardware Version: 1.1.1-303-161-103B-04 and 1.2.1-303-224-000C-03; Firmware Version: 2.13.46
3801	01/26/2021	Network Security Platform Sensor NS9500	McAfee, LLC	Hardware Version: P/N IPS-NS9500 Version 1.00 or P/N IPS-NS9500 Version 1.10; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.1
3802	01/27/2021	Juniper Networks EX4650, QFX5120 and QFX5210 Ethernet Switches	Juniper Networks, Inc	Hardware Version: EX4650-48Y-AFI, EX4650-48Y-AFO, EX4650-48Y-DC-AFI, EX4650-48Y-DC-AFO, QFX5120-32C-AFI, QFX5120-32C-AFO, QFX5120-32C-DC-AFI, QFX5120-32C-DC-AFO, QFX5120-48Y-AFI2, QFX5120-48Y-AFO2, QFX5120-48Y-DC-AFI2, QFX5120-48Y-DC-AFO2, QFX5210-64C-AFI, QFX5210-64C-AFO, QFX5210-64C-DC-AFI and QFX5210-64C-DC-AFO; Firmware Version: Junos OS 19.3R1
3803	01/28/2021	Hitachi Virtual Storage Platform (VSP) Encryption Module for NVMe	Hitachi, Ltd.	Hardware Version: P/N: 3292549-A; Version: A; Firmware Version: 90-00-01
3804	01/29/2021	PreVeil Cryptographic Module	PreVeil, Inc.	Software Version: 2.0.0