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

September 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: October 6, 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
3705	09/01/2020	Juniper Networks SRX1500, SRX4100, SRX4200 and SRX4600 Services Gateways	Juniper Networks, Inc	Hardware Version: [SRX1500 SYS-JB-AC, SRX1500 SYS-JB-DC, SRX4100 SYS-JB-AC, SRX4100 SYS-JB-DC, SRX4200 SYS-JB-AC, SRX4200 SYS-JB-DC, SRX4600 (AC), SRX4600 (DC)] with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS OS 19.2R1
3706	09/08/2020	Enovate Medical FIPS Cryptographic Module for EcoFlex, Rhythm, Envoy, and Encore	Enovate Medical LLC	Software Version: 1.0
3707	09/08/2020	MiniHSM, MiniHSM for nShield Edge F2, and MiniHSM for Time Stamp Master Clock	nCipher Security Limited	Hardware Version: nC4031Z-10, nC3021U-10, and TSMC200, Build Standard N; Firmware Version: 12.50.8
3708	09/08/2020	Mediant Session Border Controllers	AudioCodes Ltd.	Hardware Version: Mediant 4000 SBC and Mediant 9080 SBC; Firmware Version: 7.4
3709	09/14/2020	Amazon Linux 2 Kernel Crypto API Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
3711	09/21/2020	Alteryx Cryptographic Module	Alteryx Inc.	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
3712	09/22/2020	SonicWALL Network Security Virtual	SonicWall, Inc.	Firmware Version: SonicOS v6.5.4
3713	09/28/2020	Security Builder® FIPS Module	Certicom Corp.	Software Version: 5.6 [1], 5.6.1 [2] or 5.6.2 [3]
3714	09/28/2020	Extron FIPS Module	Extron Electronics	Software Version: 2.0.9 or 2.0.10
3715	09/28/2020	Security Builder® FIPS Module	Certicom Corp.	Software Version: 6.0 [1], 6.0.2 [2] and 6.0.3 [3]
3716	09/28/2020	Cisco Wireless LAN Access points 1702i, 2702e/i, 3702e/i/p, Version 8.10	Cisco Systems, Inc.	Hardware Version: 1702i, 2702e, 2702i, 3702e, 3702i and 3702p with Marvell 88W8764C with FIPS Kit: AIRLAP-FIPSKIT= VERSION A1; Firmware Version: 8.10
3717	09/28/2020	Juniper Networks NFX150 Network Services Platform	Juniper Networks, Inc.	Hardware Version: NFX150-C-S1, NFX150-S1 and NFX150-S1E; Firmware Version: Junos OS 19.2R1
3718	09/29/2020	NITROXIII CNN35XX-NFBE HSM Family	Marvell Semiconductor Inc.	Hardware Version: P/Ns CNL3560P-NFBE-G, CNL3560P-NFBE-2.0-G, CNL3560-NFBE-G, CNL3560-NFBE-2.0-G, CNL3530-NFBE-G, CNL3530-NFBE-2.0-G, CNL3510-NFBE-G, CNL3510-NFBE-2.0-G, CNL3510P-NFBE-G, CNL3510P-NFBE-2.0-G, CNN3560P-NFBE-G, CNN3560P-NFBE-2.0-G, CNN3560-NFBE-G, CNN3560-NFBE-2.0-G, CNN3530-NFBE-G, CNN3530-NFBE-2.0-G, CNN3510-NFBE-G and CNN3510-NFBE-2.0-G; Firmware Version: CNN35XX-NFBE-FW-3.4 build 07