FIPS 140-2 Consolidated Validation Certificate

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

The Communications Security Establishment of the Government of Canada

January 2018

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, 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: Michael J Cooper

Dated: 2/1/2018

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 01/02/2018

Director, Architecture and Technology Assurance
Communications Security Establishment

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3097	01/02/2018	Cisco Systems 5508 Wireless LAN Controller	Cisco Systems, Inc.	Hardware Version: 5508 with 5508 FIPS kit (AIR-CT5508FIPSKIT=); Firmware Version: 8.3
3098	01/02/2018	Cisco Systems 2504, 5520, 8510 and 8540 Wireless LAN Controllers	Cisco Systems, Inc.	Hardware Version: 2504, 5520, 8510 and 8540; Firmware Version: 8.3
3099	01/02/2018	SUSE Linux Enterprise Server - Kernel Crypto API Cryptographic Module	SUSE, LLC	Software Version: 2.0
3100	01/02/2018	Juniper Networks SRX300, SRX320, SRX340, SRX345 and SRX550-M Services Gateways	Juniper Networks, Inc.	Hardware Version: SRX300, SRX320, SRX340, SRX345, SRX550-645AP-M and SRX550-645DP-M; Firmware Version: JUNOS 15.1X49-D60
3101	01/02/2018	Juniper Networks SRX300, SRX340, and SRX345 Services Gateways	Juniper Networks, Inc.	Hardware Version: SRX300, SRX340, and SRX345 with JNPR-FIPS-TAMPER-LBLS (P/N 520-052564); Firmware Version: JUNOS 15.1X49-D60
3102	01/02/2018	WildFire WF-500	Palo Alto Networks	Hardware Version: P/N: 910-000097-00G Rev G; FIPS Kit P/N: 920-000145 Version Rev 00A; Firmware Version: 8.0.3
3103	01/05/2018	FortiWeb 5.6	Fortinet, Inc.	Firmware Version: v5.6.0, build 6180,170928
3104	01/05/2018	FortiWeb-3000E/4000E	Fortinet, Inc.	Hardware Version: C1AD49 and C1AF19 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: v5.6.0, build 6180,170928
3105	01/05/2018	ISC Cryptographic Development Kit (CDK)	Information Security Corporation	Software Version: 8.0
3106	01/09/2018	Distech SSL Cryptographic Module	Distech Controls Inc.	Firmware Version: 1.0
3107	01/09/2018	Carbon Black Cryptographic Module	Carbon Black, Inc.	Software Version: 1.0
3108	01/18/2018	NITROXIII CNN35XX-NFBE HSM Family	Cavium Inc.	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; Firmware Version: CNN35XX-NFBE-FW-3.0 build 15
3109	01/19/2018	FireEye NX Series: NX-1500, NX-2500, NX-2550, NX-3500, NX-4500, NX-5500, NX-10450	FireEye, Inc.	Hardware Version: NX-1500, NX-2500, NX-2550, NX-3500, NX-4500, NX-5500, NX-10450; Firmware Version: 8.0
3110	01/19/2018	Acme Packet 1100 and Acme Packet 3900	Oracle Communications	Hardware Version: 1100 and 3900; Firmware Version: ECz 7.5.0
3111	01/24/2018	Oracle Linux 6 NSS Cryptographic Module	Oracle Corporation	Software Version: R6-1.0.0
3112	01/25/2018	Axway Security Kernel	Axway Inc.	Software Version: 3.0.2
3113	01/26/2018	Forcepoint Java Crypto Module	Forcepoint	Software Version: 3.0.1

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3114	01/29/2018	QTI Pseudo Random Number Generator	Qualcomm Technologies, Inc.	Hardware Version: 2.1.0[1] and 2.3.1[2]
3115	01/31/2018	Panorama M-100 and M-500	Palo Alto Networks	Hardware Version: P/Ns 910-000030 Version 00D [1], 910-000092 Version 00D [1] and 910-000073 Version 00D [2]; FIPS Kit P/N 920-000140 Version 00A [1] and FIPS Kit P/N 920-000145 Version 00A [2]; Firmware Version: 8.0.3