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

December 2016

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 D Cooper

Dated: 1/12/17

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 5 Jan 2017

Director, Architecture and Technology Assurance
Communications Security Establishment

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

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
2802	12/05/2016	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: 7.1.3
2803	12/06/2016	Acronis AnyData Cryptographic Library	Acronis International GmbH	Software Version: 1.0
2804	12/08/2016	CryptoComply™ | Java	SafeLogic Inc.	Software Version: 3.0
2805	12/13/2016	Hospira CE3.0 OpenSSL Cryptographic Module	Hospira, Inc.	Software Version: 2.0.9
2806	12/13/2016	HSID5000A	KACST / Parsec	Hardware Version: HSID5000A; Firmware Version: v1.1.0
2807	12/19/2016	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (THNSB8 model)	Toshiba Corporation	Hardware Version: A0 with THNSB8480PCSE, A0 with THNSB8800PCSE, A0 with THNSB8960PCSE, A0 with THNSB81Q60CSE, or A0 with THNSB81Q92CSE; Firmware Version: 8EEF7101
2808	12/20/2016	LG OpenSSL Cryptographic Module	LG Electronics, Inc.	Software Version: 2.0.8
2809	12/20/2016	Protiva™ PIV v1.55 on TOP DL v2	Gemalto	Hardware Version: A1023378; Firmware Version: Build#11 - M1005011+ Softmask V03, Applet Version: Protiva PIV v1.55
2810	12/21/2016	EX4300 Ethernet Switches	Juniper Networks, Inc.	Hardware Version: P/N EX4300-24P, EX4300-24T, EX4300-48P, EX4300-48T, EX4300-32F with 520-052564 (Tamper Seal); Firmware Version: JUNOS 14.1X53-D30.3