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 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 Cooper

Dated: 1/30/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: January 30, 2019

for Director, Security Architecture and Risk Management
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/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3335	12/03/2018	Oracle OpenSSL FIPS Object Module	Oracle Corporation	Software Version: OpenSSL_2.0.13_OracleFIPS_1.0
3336	12/03/2018	Juniper Networks vSRX Virtual Firewall	Juniper Networks, Inc.	Software Version: Junos OS 17.4R1-S1
3337	12/04/2018	Juniper Networks SRX4600 Services Gateway	Juniper Networks, Inc.	Hardware Version: SRX4600-AC and SRX4600-DC with Tamper Seals JNPR-FIPS-TAMPER-LBLS; Firmware Version: Junos OS 18.1R1
3338	12/07/2018	CodeLathe Cryptographic Module	CodeLathe Technologies Inc.	Software Version: 18.1
3339	12/10/2018	SonicWALL SMA Series v12.1 EX-9000, SMA 6200, SMA 7200	SonicWall, Inc.	Hardware Version: EX-9000, SMA 6200 and SMA 7200; Firmware Version: 12.1.0-04493
3340	12/14/2018	SapphirePlus OpenSSL Cryptographic Module	Q Core Medical Ltd.	Software Version: 2.0.9
3341	12/17/2018	Cisco FIPS Object Module	Cisco Systems, Inc.	Software Version: 7.0
3342	12/17/2018	Oracle Linux 7 Kernel Crypto API Cryptographic Module	Oracle Corporation	Software Version: R7-2.0.0
3343	12/17/2018	Cisco Firepower Threat Defense Virtual (FTDv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.2
3344	12/17/2018	Okta Cryptographic Module for Mobile	Okta, Inc.	Software Version: 2.1
3345	12/21/2018	FlashBlade Data Encryption Module	Pure Storage, Inc.	Hardware Version: Altera ArriaV P/N 09-0001-00 and Altera ArriaX P/N 09-0208-00; Firmware Version: 71e841aae4b7bf22
3346	12/21/2018	EXP1000 Hardware Security Module	Futurex	Hardware Version: P/Ns 9850-0365 Rev10 and 9800-2082 Rev 10; Firmware Version: 6.2.0.2