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

February 2017

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: 7 Mar 2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 7 Mar 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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2827	02/01/2017	Apple iOS CoreCrypto Module v7.0	Apple Inc.	Software Version: 7.0
2828	02/01/2017	Apple iOS CoreCrypto Kernel Module v7.0	Apple Inc.	Software Version: 7.0
2829	02/01/2017	IBM(R) z/OS(R) Version 2 Release 1 System SSL Cryptographic Module	IBM Corporation	Software Version: HCPT410/JCPT411 with APAR OA50589; Hardware Version: COP chips integrated within processor unit; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 22H
2830	02/01/2017	Apple macOS CoreCrypto Kernel Module, v7.0	Apple Inc.	Software Version: 7.0
2831	02/02/2017	Oracle StorageTek T10000D Tape Drive	Oracle Corporation	Hardware Version: P/N: 7042136 and P/N: 7314405; Firmware Version: RB411111
2832	02/02/2017	Apple macOS CoreCrypto Module, v7.0	Apple Inc.	Software Version: 7.0
2833	02/03/2017	Aruba VMC-TACT Series Virtual Controllers with ArubaOS FIPS Firmware	Aruba a Hewlett Packard Enterprise Company	Firmware Version: ArubaOS VMC 6.4.2.0-1.3-FIPS
2834	02/07/2017	Aegis Secure Key 3.0 Cryptographic Module	Apricorn, Inc.	Hardware Version: RevD [ASK3-8GB (8GB), ASK3-16GB (16GB), ASK3-30GB (30GB), ASK3-60GB (60GB), ASK3-120GB (120GB), ASK3-240GB (240GB), ASK3-480GB (480GB)]; Firmware Version: 7.1
2835	02/08/2017	Apricorn FIPS Module 140-2	Apricorn, Inc.	Hardware Version: REV. D with CAN 1A; Firmware Version: 7.0
2836	02/13/2017	HiCOS PKI Applet and Taiwan TWNID Applet on NXP JCOP 3 SecID P60 (OSA)	Chunghwa Telecom Co., Ltd. and NXP Semiconductors	Hardware Version: P6022y VB; Firmware Version: JCOP 3 SECID P60 (OSA) version 0x0503.8211; Applets: HiCOS PKI Applet V1.0, TWNID Applet V1.1
2837	02/13/2017	IBM Java JCE FIPS 140-2 Cryptographic Module with CPACF	IBM Corporation	Software Version: 1.8; Hardware Version: COP chips integrated within processor unit; Firmware Version: 3863 (aka FC3863) with System Driver Level 22H
2838	02/13/2017	Command Encryption Module	Mitsubishi Space Software Co., Ltd.	Firmware Version: 3.0
2839	02/14/2017	VMware OpenSSL FIPS Object Module	VMware, Inc.	Software Version: 2.0.9
2840	02/14/2017	Arxan Cryptographic Key & Data Protection	Arxan Technologies	Software Version: 1.0

2841	02/15/2017	Cisco Adaptive Security Appliance (ASA) Virtual	Cisco Systems, Inc.	Software Version: 9.6
2842	02/17/2017	Network Security Platform Sensor NS-7100, NS-7200 and NS-7300	McAfee, Inc.	Hardware Version: P/Ns IPS-NS7100 Version 1.10, IPS-NS7200 Version 1.10 and IPS-NS7300 Version 1.10; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 8.1.17.16
2843	02/20/2017	Ciena 6500 Flex3 WaveLogic 3e OCLD Encryption Module	Ciena® Corporation	Hardware Version: 2.0 with PCB P/N NTK539QS-220; Firmware Version: 2.01
2844	02/21/2017	Centrify Cryptographic Module	Centrify Corporation	Software Version: 2.0
2845	02/22/2017	LG Kernel Loadable Cryptographic Module	LG Electronics, Inc.	Software Version: 1.0; Hardware Version: Qualcomm Snapdragon 617; Qualcomm Snapdragon 808; Qualcomm Snapdragon 820
2846	02/22/2017	Talon™ Multi-Function Security Appliance	Prometheus Security Group Global, Inc.	Hardware Version: P/Ns: TAL-SD (FIPS) v1.0 and TAL-HD (FIPS) v1.0; Firmware Version: 1.0
2847	02/22/2017	Verdasys Secure Cryptographic Module	Digital Guardian, Inc.	Software Version: 1.0
2848	02/23/2017	MICRON 1100 SSD	Micron Technology, Inc.	Hardware Version: MTFDDAK256TBN-1AR15FCHA [1], MTFDDAK512TBN-1AR15FCHA [1], MTFDDAK256TBN-1AR15FCYY [2], MTFDDAK512TBN-1AR15FCYY [2], MTFDDAV256TBN-1AR15FCHA [1], MTFDDAV512TBN-1AR15FCHA [1], MTFDDAK256TBN-1AR15FCYY [2] and MTFDDAK512TBN-1AR15FCYY [2]; Firmware Version: HPC0F10 [1] and MOMF000 [2]
2849	02/27/2017	Symantec Messaging Gateway Cryptographic Module	Symantec Corporation	Software Version: 1.0
2850	02/27/2017	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-2.0 build 68
2851	02/27/2017	Suite B Cryptographic Module	United States Special Operations Command (USSOCOM)	Software Version: v3.0.0.0