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

March 2016

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, 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: 4/1/16

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature:

Dated: APR 0 1 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2573	03/01/2016	Aruba Common Cryptographic Module	Aruba, a Hewlett Packard Enterprise company	Software Version: 1.0
2574	03/02/2016	iLO 4 Cryptographic Module	Hewlett Packard Enterprise Development LP	Hardware Version: GLP-4: 531510-004 [1], GLP-3: 531510-003 [2] and Sabine: 610107-002 [3]; Flash Memory: (820595-001 [1,2,3]); NVRAM: (820597-001 [1]), (820596-001 [2,3]); DDR3 SDRAM: (820594-001 [1,2,3]); Firmware Version: 2.11
2575	03/02/2016	Cellcrypt Secure Core 3 FIPS 140-2 Module	Cellcrypt	Software Version: 2.0.10
2576	03/02/2016	Cotap Cryptographic Module	Cotap, Inc.	Software Version: 1.0
2577	03/02/2016	Aruba Linux Cryptographic Module	Aruba, a Hewlett Packard Enterprise company	Software Version: 1.0
2578	03/07/2016	IBM Security Network Intrusion Prevention System Version 4.6.2	IBM Security	Hardware Version: GX4004, GX5008C, GX5008SFP, GX5208C, GX5208SFP, GX7412 and GX7800 with Tamper Evident Label Kit: 00VM255; Firmware Version: 4.6.2
2579	03/11/2016	QTI Inline Crypto Engine (UFS)	Qualcomm Technologies, Inc.	Hardware Version: 2.1.0
2580	03/14/2016	FireEye MX Series: MX 900, MX 8400	FireEye, Inc.	Hardware Version: MX 900, MX 8400; Firmware Version: 2.0.3
2581	03/14/2016	FireEye HX Series: HX 4400, HX 4400D, HX 4402, HX 9402	FireEye, Inc.	Hardware Version: HX 4400, HX 4400D, HX 4402, HX 9402; Firmware Version: 3.1.0
2582	03/16/2016	Red Hat Enterprise Linux 6.6 Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: 3.0
2583	03/21/2016	Box JCA Cryptographic Module	Box, Inc.	Software Version: 1.0
2584	03/21/2016	Advantech B+B SmartWorx Cryptographic Module	Advantech B+B Smartworx	Software Version: 1.0
2585	03/21/2016	VNX 6 Gb/s SAS I/O Module with Encryption from EMC	EMC Corporation	Hardware Version: 1.1.1-303-161-103B-04 and 1.2.1-303-224-000C-03; Firmware Version: 2.09.36

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2586	03/21/2016	Integral AES 256 Bit Crypto SSD Underlying PCB	Integral Memory PLC.	Hardware Version: INSSD32GS25MCR140-2(R); INSSD64GS25MCR140-2(R); INSSD128GS25MCR140-2(R); INSSD256GS25MCR140-2(R); INSSD512GS25MCR140-2(R); INSSD1TS25MCR140-2(R); INIS2564GCR140(R); INIS25128GCR140(R); INIS25256GCR140(R); INIS251TCR140(R); INIS252TCR140(R); INSSD64GS625M7CR140; INSSD128GS625M7CR140; INSSD256GS625M7CR140; INSSD512GS625M7CR140; INSSD1TS625M7CR140; INSSD2TS625M7CR140; INSSD32GS18MCR140-2(R); INSSD64GS18MCR140-2(R); INSSD128GS18MCR140-2(R); INSSD256GS18MCR140-2(R); INSSD512GS18MCR140-2(R); INSSD1TGS18MCR140-2(R); INIS1864GCR140(R); INIS18128GCR140(R); INIS18256GCR140(R); INIS18512GCR140(R); INIS181TGCR140(R); INIS182TGCR140(R); INISHS64GCR140(R); INISHS128GCR140(R); INISHS256GCR140(R); INISHS512GCR140(R); INISHS1TCR140(R); INISHS2TCR140(R); INSSD128GM2M2260C140(R); INSSD256GM2M2260C140(R); INSSD512GM2M2260C140(R); INSSD1TM2M2260C140(R); INIM26064GCR140(R); INIM260128GCR140(R); INIM260256GCR140(R); INIM260512GCR140(R); INIM2601TCR140(R); INIM2602TCR140(R); INSSD64GM2M2280C140(R); INSSD128GM2M2280C140(R); INSSD256GM2M2280C140(R); INSSD1TGM2M2280C140(R); INIM28064GCR140(R); INIM280128GCR140(R); INIM280256GCR140(R); INIM280512GCR140(R); INIM2801TCR140(R); INIM2802TCR140(R); INSSD64GMSA6MCR140(R); INSSD128GMSA6MCR140(R); INSSD256GMSA6MCR140(R); INSSD512GMSA6MCR140(R); INSSD1TMSA6MCR140(R); INIMSA64GCR140(R); INIMSA128GCR140(R); INIMSA256GCR140(R); INIMSA512GCR140(R); INIMSA1TCR140(R); INIMSA2TCR140(R); INIM24264GCR140(R); INIM242128GCR140(R); INIM242256GCR140(R); INIM242512GCR140(R); INIM2421TCR140(R); INIM2422TCR140(R); Firmware Version: S5FDM018
2587	03/21/2016	HP BladeSystem Onboard Administrator Firmware	Hewlett Packard Enterprise Development LP	Firmware Version: 4.40
2588	03/22/2016	QTI Inline Crypto Engine (SDCC)	Qualcomm Technologies, Inc.	Hardware Version: 2.1.0
2589	03/24/2016	SBC 7000 Session Border Controller	Sonus Networks, Inc.	Hardware Version: SBC 7000; Firmware Version: 5.0
2590	03/24/2016	CoSign	ARX (Algorithmic Research)	Hardware Version: 7.0; Firmware Version: 7.7
2591	03/24/2016	Network Security Platform Sensor NS-9100 and NS-9200	McAfee, Inc.	Hardware Version: P/Ns NS-9100 Versions 1.2 and 1.3 and NS-9200 Versions 1.2 and 1.3; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 8.1.17.13

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
2592	03/25/2016	Zebra DCS Cryptographic Library	Zebra Technologies Corporation	Firmware Version: DAACVS00-001-R00, DAACWS00-001-R00 or DAACUS00-001-R00
2593	03/29/2016	Network Security Platform Sensor NS-9300 S	McAfee, Inc.	Hardware Version: P/N NS-9300 S, Versions 1.2 and 1.3; FIPS Kit P/N IAC-FIPS-KT8; Firmware Version: 8.1.17.13
2594	03/29/2016	Apple iOS CoreCrypto Module v6.0	Apple Inc.	Software Version: 6.0
2595	03/29/2016	HiCOS PKI Native Smart Card Cryptographic Module	Chunghwa Telecom Co., Ltd.	Hardware Version: RS45C; Firmware Version: HardMask: 2.2 and SoftMask: 1.2
2596	03/29/2016	Network Security Platform Sensor NS-9300 P	McAfee, Inc.	Hardware Version: P/N NS-9300 P, Versions 1.2 and 1.3; FIPS Kit P/N IAC-FIPS-KT8; Firmware Version: 8.1.17.13
2597	03/29/2016	Apple OS X CoreCrypto Kernel Module v6.0	Apple Inc.	Software Version: 6.0