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

August 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 C. Cooper

Dated: 9/6/2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 06/09/2017

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
2979	08/01/2017	Cisco Adaptive Security Appliances Cryptographic Module	Cisco Systems, Inc.	Hardware Version: ASA 5506-X[1], ASA 5506H-X[1], ASA 5506W-X[1], ASA 5508-X[2][3], ASA 5512-X[2], ASA 5515-X[5], ASA 5516-X[2][4], ASA 5525-X[5], ASA 5545-X[5], ASA 5555-X[5] with [ASA5506-FIPS-KIT=][1], [ASA5500X-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3], [ASA5516-FIPS-KIT=][4] or [CISCO-FIPS-KIT=][5]; Firmware Version: 9.6
2980	08/01/2017	Security Builder FIPS Java Module	Certicom Corp.	Software Version: 2.9
2981	08/01/2017	BlackBerry Cryptographic Java Module	BlackBerry Limited	Software Version: 2.9
2982	08/03/2017	Vision ONE	bia	Hardware Version: Vision ONE Chassis P/N 991-0114-01, Vision ONE AC Power Supply P/N 991-3023-01 (QTY: 2), Vision ONE Fan Assembly P/N 991-2020-02 (QTY: 2); Firmware Version: 4.5.0.16
2983	08/03/2017	Net Tool Optimizer (NTO) 7303	bia	Hardware Version: NTO 7303 Chassis P/N 991-0082-01, NTO 7300 Series Supervisor Module P/N 992-0059-01 (QTY: 2), NTO 7300 Series Line Card with 16 QSFP+ ports P/N 992-0045-01, NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with NTO 7300 Series Advanced Feature Module Cassette with 16 SFP+ ports P/N 992-0067-01 (QTY: 2), NTO 7300 Series Carrier Line Card Hydra P/N 992-0075-01 with NTO 7300 Series 100G Port Interface Cassette P/N 992-0066-01 (QTY: 2), NTO 7300 Series Smart Blank Line Card P/N 992-0043-01, NTO 7300 Series PCM Line Card with 48 SFP+ ports P/N 992-0051-01, NTO 7300 Series ATIP Line Card with 48 SFP+ ports P/N 992-0050-01, NTO 7300 Series Fan Module Unit P/N 991-2013-01 (QTY: 6); Firmware Version: 4.5.0.16
2984	08/03/2017	Cisco FIPS Object Module	Cisco Systems, Inc.	Software Version: 6.2
2985	08/05/2017	HumanWare Kernel Cryptographic Module	Technologie Humanware	Software Version: 1.0
2986	08/10/2017	ID-One PIV on Cosmo V8.1	Oberthur Technologies	Hardware Version: P/Ns '30-5F01' [1] and '40-6001' [2]; Firmware Version: Firmware Extensions: '086294'+'086683' (ID-One PIV Applet Suite 2.4.0 on Cosmo V8.1 LARGE) [1] and Firmware Extensions: '086294'+'086693' (ID-One PIV Applet Suite 2.4.0 on Cosmo V8.1 STD) [2]
2987	08/10/2017	TRICX Cryptographic Library	Trustonic	Software Version: 1.0
2988	08/10/2017	Citrix FIPS Cryptographic Module	Citrix Systems, Inc.	Software Version: 1.0; Hardware Version: ARM v8-A, ARM v7-A, Intel Core i7 4th Generation, Intel Core i7 6th Generation, Intel Xeon 5600 series, Intel Exon E5-2600 v2 series
2989	08/10/2017	Aruba AP-324 and AP-325 Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-324-F1 (HPE SKU JW185A) and AP-325-F1 (HPE SKU JW187A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 6.5.1-FIPS
2990	08/10/2017	Aruba 2920 Switch Series	Aruba a Hewlett Packard Enterprise company	Hardware Version: J9726A and J9729A; Firmware Version: WB.16.02.0015

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
2991	08/10/2017	Samsung BoringSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.1
2992	08/14/2017	Huawei AD9430DN-24 Wireless Access Device	Huawei Technologies Co., Ltd.	Hardware Version: P/Ns AD9430DN-24 with Tamper-evident Seals 4057-113016 and External Baffles 99089JEB; Firmware Version: V200R007C10SPC100
2993	08/14/2017	Huawei AD9430DN-12 Wireless Access Device	Huawei Technologies Co., Ltd.	Hardware Version: P/Ns AD9430DN-12, Tamper Seals P/N 4057-113016; Firmware Version: V200R007C10SPC100
2994	08/14/2017	Huawei AP2030, AP4030, AP4130, AP5030, AP5130, AP6050, AP6150, AP7050 and AP8130 Wireless Access Points	Huawei Technologies Co., Ltd.	Hardware Version: P/Ns AP2030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP6050DN, AP6150DN, AP7050DE and AP8130DN with Tamper-evident Seals 4057-113016; Firmware Version: V200R007C10SPC100
2995	08/16/2017	Check Point Cryptographic Library	Check Point Software Technologies Ltd.	Firmware Version: 1.0
2996	08/18/2017	OmniSwitch AOS 8.3.1.R01 Cryptographic Module	Alcatel-Lucent Enterprise USA Inc.	Software Version: AOS 8.3.1.R01
2997	08/18/2017	CryptoComply for NSS	SafeLogic Inc.	Software Version: 4.0
2998	08/18/2017	Oracle ILOM OpenSSL FIPS Object Module	Oracle Corporation	Software Version: 2.0.10
2999	08/21/2017	Huawei R230D, R240D and R250D Remote Radio Units	Huawei Technologies Co., Ltd.	Hardware Version: P/Ns R230D, R240D and R250D with Tamper-evident Seals 4057-113016; Firmware Version: V200R007C10SPC100
3000	08/21/2017	RUGGEDCOM Ethernet Switches and RUGGEDCOM Serial Device Server	Siemens Canada Ltd.	Hardware Version: M969F, M2100F, M2200F, RSG2100F, RSG2200F, RSG2488F, RS416F, RS900F, RS900GF, and RS940GF; Firmware Version: 4.2.1.F
3001	08/23/2017	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX05S model) Type C1	Toshiba Memory Corporation	Hardware Version: A0 with PX05SMQ160B; Firmware Version: PX05AW01, PX05AW02, PX05AW03, PX05AW04

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3002	08/23/2017	HPE FlexFabric 5700, 5900 and 5920 Switch Series	Hewlett Packard Enterprise	Hardware Version: {[HPE FlexFabric 5700-32XGT-8XG-2QSFP+ Switch (JG898A), HPE FlexFabric 5700-32XGT-8XG-2QSFP+ TAA-Compliant Switch (JG899A), HPE FlexFabric 5700-40XG-2QSFP+ Switch (JG896A), HPE FlexFabric 5700-40XG-2QSFP+ TAA1-Compliant Switch (JG897A), HPE FlexFabric 5700-48G-4XG-2QSFP+ Switch (JG894A), HPE FlexFabric 5700-48G-4XG-2QSFP+ TAA1-Compliant Switch (JG895A), HPE FlexFabric 5900AF-48G-4XG-2QSFP+ Switch (JG510A), HPE FlexFabric 5900AF-48G-4XG-2QSFP+ TAA1-Compliant Switch (JH038A), HPE FlexFabric 5900AF-48XG-4QSFP+ Switch (JG772A) and HPE FlexFabric 5900AF-48XG-4QSFP+ TAA1-Compliant Switch (JG554A)] with Opacity Kit JH063A, [HPE FlexFabric 5900AF-48XGT-4QSFP+ Switch (JG336A), HPE FlexFabric 5900AF-48XGT-4QSFP+ TAA1-Compliant Switch (JH037A), HPE FlexFabric 5900CP-48XG-4QSFP+ Switch (JG838A) and HPE FlexFabric 5900CP-48XG-4QSFP+ TAA1-Compliant Switch (JH036A)] with Opacity Kit JH719A and [HPE FlexFabric 5920AF-24XG Switch (JG296A) and HPE FlexFabric 5920AF-24XG TAA1-compliant Switch (JG555A)] with Opacity Kit JG720A} with Label Kit JG585A or JG586A; Firmware Version: HPE Comware 7.1.045, Release R2422P01
3003	08/24/2017	CHR Cryptographic Module	Bull Atos Technologies	Hardware Version: 005/B; Firmware Version: V1.04-01L
3004	08/25/2017	Trusted Platform Module ST33TPHF20SPI	STMicroelectronics	Hardware Version: ST33HTPH2E28AAF0 [1], ST33HTPH2E32AAF0 [1], ST33HTPH2E28AAF1 [1], ST33HTPH2E32AAF1 [1], ST33HTPH2028AAF3 [2] and ST33HTPH2032AAF3 [2]; Firmware Version: 49.00 [1], 4A.00 [2]
3005	08/25/2017	IPCryptR2	Motorola Solutions, Inc.	Hardware Version: BLN1306A; Firmware Version: R06.03.05
3006	08/28/2017	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX05S model) Type C2	Toshiba Memory Corporation	Hardware Version: A0 with PX05SVQ096B, A0 with PX05SVQ192B, A0 with PX05SVQ384B; Firmware Version: PX05AX01, PX05AX02, PX05AX03, PX05AX04
3007	08/28/2017	CryptoComply for Libgcrypt	SafeLogic Inc.	Software Version: 4.0
3008	08/31/2017	Fatpipe Crypto Module	Fatpipe, Inc.	Software Version: 9.1.2-fips