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

May 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: 6/8/17

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: JUN 0 6 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
2895	05/02/2017	Cisco Aironet 1532e/i, 1552e/i, 1572 EAC, 1602e/i, 1702i, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p, 3702e/i/p and IW3702-2E/4E Wireless LAN Access Points	Cisco Systems, Inc.	Hardware Version: 1532e[5], 1532i[5], 1552e[2], 1552i[2], 1572 EAC[4], 1602e[3], 1602i[3], 1702i[4], 2602e[4], 2602i[4], 2702e[4], 2702i[4], 3502e[2], 3502i[2], 3602e[4], 3602i[4], 3602p[4], 3702e[4], 3702i[4], 3702p[4], 3602e[1,4], 3602i[1,4], 3602p[1,4], 3702e[1,4], 3702i[1,4], 3702p[1,4], IW3702-2E[4] and IW3702-4E[4] with AIR-RM3000M[1], Marvell 88W8364[2], Marvell 88W8763C[3], Marvell 88W8764C[4] and Qualcomm Atheros AES-128w10i[5]) with FIPS Kit: AIRLAP-FIPSKIT=, VERSION B0; Firmware Version: 8.3
2896	05/03/2017	Pulse Secure Cryptographic Module	Pulse Secure, LLC	Software Version: 2.0
2897	05/04/2017	Cisco Firepower Management Center Cryptographic Modules	Cisco Systems, Inc.	Hardware Version: FS750-K9, FS1500-K9, FS2000-K9, FS3500-K9 and FS4000-K9; Firmware Version: 6.1
2898	05/04/2017	Cisco ASA Cryptographic Module	Cisco System, Inc.	Hardware Version: FPR4110-ASA-K9, FPR4120-ASA-K9, FPR4140-ASA-K9, FPR4150-ASA-K9, FPR9K-SM-24 (SM-24) and FPR9K-SM-36 (SM-36); Firmware Version: 9.6
2899	05/04/2017	Cisco Firepower Management Center Virtual (FMCv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.1
2900	05/05/2017	SAP CommonCryptoLib Crypto Kernel	SAP SE	Software Version: 8.4.47.0 32-bit [1] and 64-bit [2]
2901	05/08/2017	Huawei AR1200 and AR2200 Series Routers	Huawei Technologies Co., Ltd.	Hardware Version: AR1220E P/N 02350DQJ Version E.5 with [1], AR1220EVW P/N 02350DQL Version F.5 with [1] and AR2220E P/N 02350DQM Version E.6 with [1]; Tamper Evident Seals P/N 4057-113016 [1]; Firmware Version: V200R008C10SPC110
2902	05/09/2017	Cisco Firepower Next-Generation IPS Virtual (NGIPSv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.1
2903	05/10/2017	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX05S model) Type B1	Toshiba Corporation	Hardware Version: A2 with PX05SVQ040B, A2 with PX05SRQ192B, A2 with PX05SRQ384B; Firmware Version: PX05PD43

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
2904	05/10/2017	Brocade(R) NetIron(R) CER 2000 Series Ethernet Routers and Brocade NetIron(R) CES 2000 Series Ethernet Switches	Brocade Communications Systems, Inc.	Hardware Version: {[BR-CER-2024C-4X-RT-AC (80-1006530-01) with RPS9 (80-1003868-01) and SW-CER-2024-RTUPG (80-1004848-01), BR-CER-2024C-4X-RT-DC (80-1007213-01) with RPS9DC (80-1003869-02) and SW-CER-2024-RTUPG (80-1004848-01), BR-CER-2024F-4X-RT-AC (80-1006529-01) with RPS9 (80-1003868-01) and SW-CER-2024-RTUPG (80-1004848-01), BR-CER-2024F-4X-RT-DC (80-1007212-01) with RPS9DC (80-1003869-02) and SW-CER-2024-RTUPG (80-1004848-01)], [BR-CES-2024C-4X-AC (80-1000077-01) with RPS9 (80-1003868-01), BR-CES-2024C-4X-DC (80-1007215-01) with RPS9DC (80-1003869-02), BR-CES-2024F-4X-AC (80-1000037-01) with RPS9 (80-1003868-01), BR-CES-2024F-4X-DC (80-1007214-01) with RPS9DC (80-1003869-02)]} with FIPS Kit XBR-000195; Firmware Version: Multi-Service IronWare R06.0.00aa
2905	05/10/2017	Becrypt Cryptographic Library	Becrypt Limited	Software Version: 3.0; Hardware Version: Intel Core i5-4300Y
2906	05/10/2017	Ubuntu OpenSSH Server Cryptographic Module	Canonical Ltd.	Software Version: 1.0
2907	05/10/2017	Ubuntu OpenSSH Client Cryptographic Module	Canonical Ltd.	Software Version: 1.0
2908	05/13/2017	Hewlett Packard Enterprise NSS Crypto Module	Hewlett Packard Enterprise	Software Version: 4.0
2909	05/15/2017	Arista Networks OpenSSL Module	Arista Networks, Inc.	Software Version: openssl-1.0.2h-fips
2910	05/15/2017	Huawei S12700 Series Switches	Huawei Technologies Co., Ltd.	Hardware Version: S12704 P/N 02114480 Version E.3, S12708 P/N 02114178 Version Q.3 and S12712 P/N 02114180 Version P.3 all with MPU P/N 03030RPE, SFU P/N 03030RPF, LPU P/N 03030SGN and Tamper Seals P/N 4057-113016; Firmware Version: V200R010C00SPC900B900
2911	05/15/2017	Cryptographic Module for BIG-IP®	F5 Networks	Software Version: 12.1.2 HF1
2912	05/16/2017	Unity 12 Gb/s SAS I/O Module with Encryption	EMC Corporation	Hardware Version: Storage Processor SAS Module with P/N 362-000-332, P/N 363-000-071, P/N 363-000-084 and P/N 364-000-096 and Pluggable I/O SAS Module with P/N 362-000-333, P/N 363-000-071, P/N 363-000-084 and P/N 364-000-063; Firmware Version: 03.90
2913	05/24/2017	Mocana Cryptographic Loadable Kernel Module	Mocana Corporation	Software Version: 6.4.1f
2914	05/26/2017	Huawei S6720EI Series Switches	Huawei Technologies Co., Ltd.	Hardware Version: P/Ns 02350DMN Version H.3 (S6720-30C-EI-24S-AC) and 02350DMP Version H.3 (S6720-54C-EI-48S-AC) both with P/Ns 4057-113016 (Tamper Evident Seals) and 99089JEB (External Baffle); Firmware Version: V200R010C00SPC900B900
2915	05/30/2017	Hewlett Packard Enterprise libgcrypt Crypto Module	Hewlett Packard Enterprise	Software Version: 4.0

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
2916	05/30/2017	Kaspersky Cryptographic Module (Pre-Boot)	Kaspersky Lab UK Ltd.	Software Version: 3.0.1.25
2917	05/30/2017	GSP3000 Hardware Security Module	Futurex	Hardware Version: P/N 9800-2079 Rev7; Firmware Version: 6.2.0.0
2918	05/30/2017	Viptela Cryptographic Module	Viptela	Software Version: 2.1