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

October 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: 11/1/2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [signature]

Dated: 1 NOV 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

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
2762	10/03/2016	Evolution e8350-FIPSL2 Satellite Router Board [1], iConnex e800-FIPSL2 Satellite Router Board [2], iConnex e850MP-FIPSL2 Satellite Router Board [3], Evolution eM1D1-FIPSL2 Line Card [4], and Evolution eM0DM-FIPSL2 Line Card [5]	VT iDirect, Inc.	Hardware Version: E0000051-0005 [1], E0001340-0001 [2], E0000731-0004 [3], E0001306-0001 [4], and E0001306-0002 [5]; Firmware Version: iDX 3.3.2.5
2763	10/06/2016	IBM(R) z/OS(R) Version 2 Release 1 ICSF PKCS #11 Cryptographic Module	IBM Corporation	Software Version: OA50113; Hardware Version: COP chips integrated within processor unit [1] and P/N 00LV487 [2]; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 22H [1] and CCA 5.2.27z RC30 [2]
2764	10/06/2016	nShield Remote Administration Token	Thales e-Security Inc.	Hardware Version: NXP P60D144; Firmware Version: Athena IDProtect 0501.5175.0001 with Authentication Token Applet 1.0
2765	10/07/2016	FortiOS 5.2	Fortinet, Inc.	Firmware Version: 5.2.7, build0718,160328
2766	10/11/2016	Samsung SAS 12G TCG Enterprise SSC SEDs PM163x Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILS3T8HCJM-000G6; Firmware Version: NA02
2767	10/11/2016	Kaspersky Cryptographic Module (Kernel Mode)	Kaspersky Lab UK Ltd.	Software Version: 3.0.1.25
2768	10/12/2016	BC-FJA (Bouncy Castle FIPS Java API)	Legion of the Bouncy Castle Inc.	Software Version: 1.0.0
2769	10/13/2016	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type C	Toshiba Corporation	Hardware Version: A0 with PX04SMQ080B or PX04SMQ160B; Firmware Version: AR02

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
2770	10/17/2016	Brocade VDX 6740, VDX 6740T, VDX 6940 and VDX 8770 Switches	Brocade Communications Systems, Inc.	Hardware Version: {[BR-VDX6740-24-F (80-1007295-01), BR-VDX6740-24-R (80-1007294-01), BR-VDX6740-48-F (80-1007483-01), BR-VDX6740-48-R (80-1007481-01), BR-VDX6740-64-F (80-1007520-01) and BR-VDX6740-64-R (80-1007521-01)], [BR-VDX6740T-24-F (80-1007273-01), BR-VDX6740T-24-R (80-1007274-01), BR-VDX6740T-48-F (80-1007485-01), BR-VDX6740T-48-R (80-1007487-01), BR-VDX6740T-64-F (80-1007522-01), BR-VDX6740T-64-R (80-1007523-01), BR-VDX6740T-56-1G-R (80-1007863-03) and BR-VDX6740T-56-1G-F (80-1007864-03)], [BR-VDX6940-24Q-AC-F (80-1008854-01), BR-VDX6940-24Q-AC-R (80-1008855-01), BR-VDX6940-36Q-AC-F (80-1008851-01), BR-VDX6940-36Q-AC-R (80-1008850-01), BR-VDX6940-64S-AC-F (80-1008529-01), BR-VDX6940-64S-AC-R (80-1008526-01), BR-VDX6940-96S-AC-F (80-1008530-01), BR-VDX6940-96S-AC-R (80-1008527-01), BR-VDX6940-144S-AC-F (80-1008531-01), BR-VDX6940-144S-AC-R (80-1008528-01)], [BR-VDX8770-4-BND-AC (80-1005850-02), BR-VDX8770-4-BND-DC (80-1006532-03), BR-VDX8770-8-BND-AC (80-1005905-02) and BR-VDX8770-8-BND-DC (80-1006533-03)] with FRUs (80-1006430-01, 80-1006295-01, 80-1006294-02, 80-1006293-02, 80-1006048-02, 80-1006431-01, 80-1006429-01)} with FIPS Kit P/N Brocade XBR-000195 (80-1002006-02); Firmware Version: Network OS (NOS) v6.0.2 P/N: 63-1001691-01
2771	10/17/2016	Cisco Catalyst 4506-E with Supervisor Card (WS-X45-SUP8-E) and Line Cards (WS-X4748-RJ45-E and WS-X4748-RJ45V+E)	Cisco Systems, Inc.	Hardware Version: WS-C4506-E with Supervisor card [WS-X45-SUP8-E] and Line cards [WS-X4748-RJ45V+E and WS-X4748-RJ45-E]; Firmware Version: IOS-XE 3.7.0E
2772	10/18/2016	Rosetta microSDHC(TM)	SPYRUS, Inc.	Hardware Version: 851314011F, 851314012F and 851314013F; Firmware Version: 3.0.2
2773	10/19/2016	Protiva PIV Applet v1.55 on Protiva TOP DL Card	Gemalto	Hardware Version: A1005291- CHIP.P5CD144.MPH051B, A1011108 - CHIP.P5CD144.MPH051B and A1047808 -CHIP.P5CD144.MPH051B; Firmware Version: GX4-FIPS EI08, Applet Version: Protiva PIV Applet v1.55
2774	10/19/2016	SafesITe TOP DL GX4 - FIPS with ActivIdentity Digital Identity Applet Suite V2 for Extended PIV	Gemalto and ActivIdentity Inc.	Hardware Version: A1005291 - CHIP.P5CD144.MPH051B, A1011108 - CHIP.P5CD144.MPH051B and A1047808 - CHIP.P5CD144.MPH051B; Firmware Version: GX4-FIPS EI08, Applet Versions: ACA applet package v2.6.2B.4, ASC library package v2.6.2B.3, PKI/GC/SKI applet package v2.6.2B.4, PIV End Point Wrapper module v2.6.2B.4, PIV End Point Extended module v2.6.2B.3, SMA applet package v2.6.2B.3
2775	10/20/2016	Cisco Cloud Services Router 1000 Virtual	Cisco Systems, Inc.	Software Version: 3.16
2776	10/21/2016	FX Cryptographic Kernel Module	Fuji Xerox Co., Ltd.	Software Version: 1.0.3

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
2777	10/21/2016	BlackBerry Cryptographic Java Module	BlackBerry Limited	Software Version: 2.8 [1], 2.8.7 [1], 2.8.8 [2], 2.9 [2]
2778	10/24/2016	Security Builder FIPS Java Module	Certicom Corp.	Software Version: 2.8 [1], 2.8.7 [1], 2.8.8 [2], 2.9 [2]
2779	10/25/2016	DocuSign Signature Appliance	DocuSign, Inc.	Hardware Version: 8.0; Firmware Version: 8.1
2780	10/31/2016	Red Hat Enterprise Linux GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: 4.0
2781	10/31/2016	FortiGate-100D/200D/300D/500D	Fortinet, Inc.	Hardware Version: C4LL40, C4KV72, C1AB49 and C1AB51 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: 5.2.7, build0718, 160328
2782	10/31/2016	FortiGate-3700D/3815D	Fortinet, Inc.	Hardware Version: C1AA92 and C1AE66 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: 5.2.7, build0718, 160328
2783	10/31/2016	FortiGate-1000D/1500D	Fortinet, Inc.	Hardware Version: C1AB95 and C1AA64 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: 5.2.7, build0718, 160328
2784	10/31/2016	FortiGate-30D/60D/92D, FortiWiFi-60D and FortiGateRugged-60D	Fortinet, Inc.	Hardware Version: C1AA93, C1AB28, C1AC34, C1AB32, and C1AB57 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: 5.2.7, build0718,160328