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

July 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 A Cooper

Dated: 4 Aug 2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature:

Dated: 4 Aug 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2670	07/04/2016	FibeAir® IP-20C, FibeAir® IP-20S, FibeAir® IP-20N, FibeAir® IP-20A, FibeAir® IP-20G, and FibeAir® IP-20GX	Ceragon Networks, Ltd.	Hardware Version: IP-20N, IP-20A, IP-20G, IP-20GX, IP-20C, IP-20S, IP-20-TCC-B-MC+SD-AF: 24-T009-1|A, IP-20-TCC-B2+SD-AF: 24-T010-1|A, IP-20-TCC-B2-XG-MC+SD-AF: 24-T011-1|A, IP-20-RMC-B-AF: 24-R010-0|A; Firmware Version: CeraOS 8.3
2671	07/07/2016	Duo Security Cryptographic Module	Duo Security, Inc.	Software Version: 1.0
2672	07/07/2016	IAS Router	Information Assurance Specialists, Inc.	Hardware Version: P/Ns IAS STEW Rev 1.0, IAS KG-RU Rev 1.0 and IAS Router Micro Rev 1.0; Firmware Version: 50e8756 - 2015-11-24
2673	07/08/2016	LX-4000T Series Console Servers	MRV Communications Inc.	Hardware Version: 600-R3265 RevB through 600-R3288 RevB (inclusive), 600-R3265 RevC through 600-R3288 RevC (inclusive), 600-R3265 RevD through 600-R3288 RevD (inclusive) and 600-R3265 RevE through 600-R3288 RevE (inclusive); Firmware Version: LinuxITO Version: 6.1.0 and PPCiboot Version: 5.3.9
2674	07/11/2016	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: SKC1.7
2675	07/11/2016	Cisco Optical Networking Solution (ONS) 15454 Multiservice Transport Platforms (MSTPs) & NCS 2000 Series	Cisco Systems, Inc.	Hardware Version: [15454-M2-SA, 15454-M6-SA, NCS2002-SA, NCS2006-SA, NCS2015-SA, 15454-M-TNC-K9, 15454-M-TSC-K9, 15454-M-TNCE-K9, 15454-M-TSCE-K9, NCS2K-TNCS-O-K9, NCS2K-TNCS-K9, 15454-M-WSE-K9, NCS2K-MR-MXP-LIC, 15454-M-10X10G-LC, and NCS2K-200G-CK-LIC] with FIPS Kit: CISCO-FIPS-KIT=; Firmware Version: 10.5
2676	07/11/2016	Cohesity OpenSSL FIPS Object Module	Cohesity, Inc.	Software Version: 1.0.1
2677	07/15/2016	SMA 6200 and SMA 7200	Dell Software, Inc.	Hardware Version: P/Ns 101-500399-57 Rev A and 101-500398-57 Rev A; Firmware Version: SRA 10.7.2-619
2678	07/15/2016	Johnson Encryption Machine 2 (JEM2)	EFJohnson Technologies	Hardware Version: P/Ns R035-3900-180-00 and R035-3900-280-01; Firmware Version: 4.1
2679	07/15/2016	MultiApp V31 Platform	Gemalto SA	Hardware Version: NXP P60D080P VC (MPH132), NXP P60D144P VA (MPH149); Firmware Version: MultiApp V31 patch 1.4, Demonstration Applet version V1.3
2680	07/15/2016	LG Kernel Cryptographic Module	LG Electronics, Inc.	Software Version: 3.4.0 [1] or 3.10.49 [2, 3]
2681	07/15/2016	Brocade(R) NetIron(R) CER 2000 Ethernet Routers and Brocade CES 2000 Routers and Switches	Brocade Communications Systems, Inc.	Hardware Version: {[BR-CER-2024C-4X-RT-AC (80-1006530-01), BR-CER-2024C-4X-RT-DC (80-1007213-01), BR-CER-2024F-4X-RT-AC (80-1006529-01), BR-CER-2024F-4X-RT-DC (80-1007212-01), RPS9 (80-1003868-01) and RPS9DC (80-1003869-02)], [BR-CES-2024C-4X-AC (80-1000077-01), BR-CES-2024C-4X-DC (80-1007215-01), BR-CES-2024F-4X-AC (80-1000037-01), BR-CES-2024F-4X-DC (80-1007214-01), RPS9 (80-1003868-01) and RPS9DC (80-1003869-02)]} with FIPS Kit XBR-000195; Firmware Version: Multi-Service IronWare R05.8.00a

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
2682	07/19/2016	Cisco Integrated Services Router (ISR) 1905 ISR, 1921 ISR, 1941 ISR, 2901 ISR, 2911 ISR, 2921 ISR, 2951 ISR, 3925 ISR, 3925E ISR, 3945 ISR, 3945E ISR, 5915 ESR and 5940 ESR	Cisco Systems, Inc.	Hardware Version: 1905, 1921, 1941 [3], 2901 [4], 2911 [5], 2921 [6], 2951 [7], 3925 [8], 3945 [9], 3925E [10], 3945E [11], 5915, 5940 with PVDM2-8 [4, 5, 6, 7, 8, 9, 10, 11], PVDM2-16 [4, 5, 6, 7, 8, 9, 10, 11], PVDM2-32 [4, 5, 6, 7, 8, 9, 10, 11], PVDM2-48 [4, 5, 6, 7, 8, 9, 10, 11], PVDM2-64 [4, 5, 6, 7, 8, 9, 10, 11], PVDM3-16 [4, 5, 6, 7, 8, 9, 10, 11], PVDM3-32 [4, 5, 6, 7, 8, 9, 10, 11], PVDM3-64 [4, 5, 6, 7, 8, 9, 10, 11], PVDM3-128 [4, 5, 6, 7, 8, 9, 10, 11], PVDM3-192 [4, 5, 6, 7, 8, 9, 10, 11], PVDM3-256 [4, 5, 6, 7, 8, 9, 10, 11] and ISM-VPN-19 [3], ISM-VPN-29 [4, 5, 6, 7], ISM-VPN-39 [8, 9]; Firmware Version: IOS 15.5M
2683	07/19/2016	Cisco Integrated Services Router (ISR) 891W, 1941W, 829W	Cisco Systems, Inc.	Hardware Version: C891FW-A, C891FW-E, 1941W, IR829GW-LTE-NA-A, IR829GW-LTE-VZ-A; Firmware Version: Router IOS 15.5M and AP IOS 15.3.3-JB
2684	07/19/2016	Cisco C819 ISR, C880 ISR, C890 ISR, CGR 2010, C800M, ESR5921, and IR809	Cisco Systems, Inc.	Hardware Version: C819G-4G-GA, C819G-4G-NA, C819G-4G-ST, C819G-4G-VZ, C819HG-4G-A, C819HG-4G-G, C819HG-4G-V, ESR5921, C881, C881G-4G-GA, C887VAG-4G-GA, C891F, C892FSP, C897VA, C897VAG-LTE-GA, C899G-LTE-GA, C899G-LTE-NA, C899G-LTE-ST, C899G-LTE-VZ, CGR 2010 [1], C841M-4X, C841M-8X, IR809G-LTE-VZ, IR809G-LTE-NA with GRWIC-ESM-8x [1] or GRWIC-ESM-4x [1]; Firmware Version: IOS 15.5M
2685	07/19/2016	SPYRUS USB-3 Module	SPYRUS Inc.	Hardware Version: SFP100000-1; SFP100000-2; SFP100000-3; SFP100000-4; SFP200000-1; SFP200000-2; SFP200000-3; SFP200000-4; SFP300000-1; SFP300000-2; SFP300000-3; SFP300000-4; Firmware Version: 3.0.2
2686	07/19/2016	Voltage Cryptographic Module v.5.0	HPE Data Security	Software Version: Version 5.0
2687	07/25/2016	SyncDog Cryptographic Module	SyncDog, Inc.	Software Version: 2.5
2688	07/26/2016	datAshur Pro 3.0	iStorage Limited	Software Version: N/A; Hardware Version: IS-FL-DA3-256-8; IS-FL-DA3-256-16; IS-FL-DA3-256-32; IS-FL-DA3-256-64; Firmware Version: Encryption Controller: MPALL_F1_6600_v384_0A-0002; Security Controller: v1.11
2689	07/27/2016	Kaminario Encryption Module	Kaminario	Software Version: 1.0
2690	07/28/2016	MX240, MX480, and MX960 3D Universal Edge Routers with the Multiservices MPC and Junos 14.2X4-D10.7	Juniper Networks, Inc.	Hardware Version: MX240, MX480 and MX960 with components identified in Security Policy Table 1; Firmware Version: Junos 14.2X4-D10.7
2691	07/28/2016	IBM(R) z/OS(R) Version 2 Release 1 Security Server RACF(R) Signature Verification Module version 1.0	IBM Corporation	Software Version: RACF level HRF7790; Hardware Version: FC 3863 EC N98775 Drv 22H
2692	07/28/2016	HSM-ZJ2014	Zanjia Electronic Science & Technology (Beijing) Co., Ltd.	Hardware Version: ZJ2014-2697v2-680-32G; Firmware Version: 1.0.0.1