FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

TM

The Communications Security Establishment of the Government of Canada

March 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 Cooper

Dated: 4/3/2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: APR 0 3 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
2852	03/01/2017	CTERA Crypto Module™ (Java)	CTERA Networks Ltd.	Software Version: 3.0
2853	03/02/2017	Kaspersky Cryptographic Module (User Mode)	Kaspersky Lab UK Ltd.	Software Version: 3.0.1.25
2854	03/02/2017	Communication Cryptographic Library (CCL)	EFJohnson Technologies	Software Version: Product Number 039-5804-200 Rev 3.0
2855	03/03/2017	CryptoMod	Automation Solutions, Inc	Hardware Version: CM5705-D9; Firmware Version: 1.0.51.FIPS
2856	03/07/2017	Juniper Networks SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways	Juniper Networks, Inc.	Hardware Version: P/Ns {SRX100H2, SRX110H2-VA, SRX110H2-VB, SRX210HE2, SRX220H2, SRX240H2, SRX550, SRX650} with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS-FIPS 12.3X48-D30
2857	03/08/2017	Motorola Network Router (MNR) S6000	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1780L Rev FB with Encryption Module P/N CLN8261D Rev NA; Firmware Version: GS-16.9.0.48
2858	03/08/2017	Motorola GGM 8000 Gateway	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1841F Rev AB with FIPS Kit P/N CLN8787A Rev B and Power Supply P/N CLN1850A Rev G (AC) or P/N CLN1849C Rev AA (DC); Firmware Version: KS 16.9.0.48
2859	03/08/2017	Mocana Cryptographic Suite B Module	Mocana Corporation	Software Version: 6.4.1f
2860	03/08/2017	DocuSign HSM Appliance	DocuSign, Inc.	Hardware Version: 5.0; Firmware Version: 5.0.0
2861	03/15/2017	Dell Crypto Library for Dell iDRAC and Dell CMC	Dell, Inc.	Software Version: 2.4
2862	03/10/2017	HPE Enterprise Secure Key Manager	Hewlett Packard Enterprise	Software Version: N/A; Hardware Version: P/N M6H81AA , Version 5.0; Firmware Version: 7.0.1
2863	03/16/2017	WatchGuard Firebox M200[1], M300[2], M400[3], M500[4], M440[5], M4600[6], M5600[7]	WatchGuard Technologies, Inc.	Hardware Version: ML3AE8 [1,2]; SL1AE24 [5]; KL5AE8 [3,4]; CL4AE24 [6] with WG8583, WG8584 and WG8597; CL5AE32 [7] with WG8583, WG8584, WG8585, WG8022, and WG8598; FIPS Kit P/N: WG8566; Firmware Version: Fireware OS v11.11.2

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
2864	03/21/2017	Brocade(R) MLXe(R) Series Ethernet Routers, 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-MLXE-8-MR2-M-AC (80-1007225-01), BR-MLXE-16-MR2-M-AC (80-1006827-02), BR-MLXE-32-MR2-M-AC (80-1007253-04), BR-MLXE-4-MR2-X-AC (80-1006874-03), BR-MLXE-32-MR2-X-AC (80-1007255-04), with Components (80-1005643-01, 80-1005644-03, 80-1005641-02, 80-1005642-03, 80-1007878-02, 80-1007911-02, 80-1008426-01, 80-1008427-02, 80-1007879-02, 80-1003891-02, 80-1002983-01, 80-1008686-01, 80-1003971-01, 80-1003969-02, 80-1004114-01, 80-1004113-01, 80-1004112-01, 80-1004469-01, 80-1004760-02, 80-1006511-02, 80-1004757-02, 80-1003009-01, 80-1003052-01, 80-1003053-01)], [BR-CER-2024C-4X-RT-AC (80-1006530-01), BR-CER-2024F-4X-RT-AC (80-1006529-01), with Components (80-1003868-01, 80-1004848-01)], [BR-CES-2024C-4X-AC (80-1000077-01), BR-CES-2024F-4X-AC (80-1000037-01), with Component (80-1003868-01)]} with FIPS Kit XBR-000195; Firmware Version: Multi-Service IronWare R05.9.00aa
2865	03/21/2017	Brocade(R) DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones, 6510 and 6520 FC Switches, and 7800 Extension Switch	Brocade Communications Systems, Inc.	Hardware Version: {6510 FC Switch (P/N 80-1005272-03) with FRU (P/N 80-1001304-02) with Software License (P/N 80-1005356-02), 6520 FC Switch (P/N 80-1007257-03) with FRUs (P/Ns 80-1007263-01 and 80-1004580-02) with Software License (P/N 80-1007272-01), 7800 Extension Switch (P/N 80-1006977-02) with Software License (P/N 80-1002820-02); [DCX Backbone (P/N 80-1006752-01), DCX-4S Backbone (P/N 80-1006772-01), DCX 8510-4 Backbone (P/N 80-1006964-01), DCX 8510-8 Backbone (P/N 80-1007025-01)] with Blades (P/Ns 80-1006794-01, 80-1004897-01, 80-1004898-01, 80-1006771-01, 80-1006750-01, 80-1005166-02, 80-1005187-02, 80-1006936-01, 80-1006779-01, 80-1006823-01, 80-1007000-01, 80-1007017-01, 49-1000016-04, 49-1000064-02 and 49-1000294-05)} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v7.4.0 (P/N 51-1001672-01)
2866	03/22/2017	VMware Java JCE (Java Cryptographic Extension) Module	VMware, Inc.	Software Version: 2.0
2867	03/23/2017	HPE LTO-6 Tape Drive	Hewlett Packard Enterprise	Hardware Version: P/Ns AQ278A #912 [1], AQ288D #103 [2] and AQ298C #103 [3]; Firmware Version: J5SW [1], 35PW [2] and 25MW [3]
2868	03/24/2017	Tavve Cryptographic Module	Tavve Software Company	Software Version: 6.0

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
2869	03/27/2017	Aviat Networks Eclipse Cryptographic Module	Aviat Networks, Inc.	Hardware Version: INUe 2RU Chassis (P/N EXE-002), Fan Card (P/N EXF-101), Node Controller Card (P/N EXN-004 with FPGA_NCCV2_E1_DS1_004.bit and FPGA_NCCV2_STM1_006.bit), FIPS Installation Kit (P/N 179-530153-001 or 179-530153-002), Replacement Labels (P/N 007-600331-001), at least one of: [RAC 6X (P/N EXR-600-001 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 6XE (P/N EXR-600-002 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 60 (P/N EXR-660-001 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit), or RAC 60E (P/N EXR-660-002 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit)] and all remaining slots filled by excluded components as specified in the Security Policy.; Firmware Version: 08.02.91 with Bootloader version 1.0.36
2870	03/28/2017	INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit	INTEGRITY Security Services	Firmware Version: 3.0.3
2871	03/28/2017	VMAX 12 Gb/s SAS I/O Module with Encryption	Dell EMC	Hardware Version: 303-305-100A-06; Firmware Version: v3.08.41.00
2872	03/30/2017	Veeam Cryptographic Module	Veeam Software Corporation	Software Version: 2.1