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

Consolidated Certificate No. 0057

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: 10/1/2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Greg Wilts

Signature:

Dated: OCT 0 1 2015

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2438	09/03/2015	Alcatel-Lucent 1830 Photonic Service Switch (PSS)	Alcatel-Lucent	Hardware Versions: WOCUATAUAB / 3KC12841AA 02 [1], WOM3P00CRC / 8DG59859AA 03 [2], WOMNW00ERB / 8DG59319AA 02 [3], EC PSS-4 (3KC-12828-ABAC) [1], E4PFDCAK [1], 11QPEN4 [1-3], 10G MR XFP [1-3], 10GBASE-SR XFP [1-3], 1AB396080001 [1-3], X8FCLC-L [1-3], X8FCSN-I [1-3], XL-64TU XFP [1-3], EC PSS-16/PSS-32 (8DG59241AD) [2,3], PF (-48V DC) PSS-16, 20A [2], 8DG-59418-AA [1-3], PF (-48V DC) PSS-32, 20A [3], 8DG-61258-GAAA-TSZZA [3], with FIPS Kits 3KC-13452-AAAA [1], 3KC-13453-AAAA [1], 8DG-62678-AAAA [2] and 8DG-62677-AAAA [3]; Firmware Version: 1.3.1
2439	09/03/2015	NPCT6XX TPM 1.2	Nuvoton Technology Corporation	Hardware Versions: FB5C85D IN TSSOP28 PACKAGE and FB5C85D IN QFN32 PACKAGE; Firmware Version: 5.81.0.0
2440	09/03/2015	Java Card Platform for Infineon on SLE 78 (SLJ 52GxxyyyzR)	Oracle Corporation	Hardware Version: M7892 B11; Firmware Version: 1.0f
2441	09/08/2015	Red Hat Enterprise Linux 6.6 OpenSSL Module	Red Hat®, Inc.	Software Version: 3.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2442	09/09/2015	Kanguru Defender Elite300	Kanguru Solutions	Hardware Versions: P/Ns KDFE300-4G-Green, KDFE300-4G-Black, KDFE300-4G-Red, KDFE300-4G-Silver, KDFE300-8G-Green, KDFE300-8G-Black, KDFE300-8G-Red, KDFE300-8G-Silver, KDFE300-16G-Green, KDFE300-16G-Black, KDFE300-16G-Red, KDFE300-16G-Silver, KDFE300-32G-Green, KDFE300-32G-Black, KDFE300-32G-Red, KDFE300-32G-Silver, KDFE300-64G-Green, KDFE300-64G-Black, KDFE300-64G-Red, KDFE300-64G-Silver, KDFE300-128G-Green, KDFE300-128G-Black, KDFE300-128G-Red, KDFE300-128G-Silver, Version 1.0; Firmware Version: 2.10.10
2443	09/09/2015	Pitney Bowes MS1 X4 Postal Security Device (PSD)	Pitney Bowes, Inc.	Hardware Versions: Part # 4W84001 Rev AAA; MAX32590 Secure Microcontroller Revision B4; Firmware Version: Device Abstraction Layer (DAL) Version 01.01.00F4; PB Bootloader Version 00.00.0016; PSD Application Version 21.04.807E
2444	09/14/2015	Lexmark™ Crypto Module	Lexmark International, Inc.	Firmware Version: 2.10
2445	09/15/2015	Accellion kiteworks Cryptographic Module	Accellion, Inc.	Software Version: KWLIB_2_0_2
2446	09/16/2015	Red Hat Enterprise Linux 6.6 OpenSSH Server Cryptographic Module	Red Hat®, Inc.	Software Version: 3.0
2447	09/16/2015	Red Hat Enterprise Linux 6.6 OpenSSH Client Cryptographic Module	Red Hat®, Inc.	Software Version: 3.0
2448	09/17/2015	Vectra Networks Cryptographic Module	Vectra Networks	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2449	09/23/2015	Cobham AES Cryptographic Firmware-Hybrid Module	Cobham TCS Limited	Hardware Version: Freescale ColdFire MCF54453; Firmware Version: 1.0
2450	09/23/2015	Samsung SAS 12G TCG Enterprise SSC SED PM1633	Samsung Electronics Co., Ltd.	Hardware Versions: MZILS960HCHP-000H9; MZILS1T9HCHP-000H9; MZILS3T8HCJM-000H9; Firmware Version: 3P00
2451	09/30/2015	Juniper Networks RE1800 and RE2600 Routing Engines Cryptographic Modules	Juniper Networks, Inc.	Hardware Versions: P/Ns RE-S-1800X2-XXG, RE-S-1800X4-XXG, RE-S-EX9200-1800X4-XXG, RE-DUO-C1800-16G, RE-B-1800X1-4G, RE-A-1800X2-XXG, RE-DUO-C2600-16G, 520-052564; Firmware Version: Junos 14.1R4 with Junos FIPS mode utilities 14.1R4
2452	09/30/2015	Atalla Cryptographic Subsystem (ACS)	Hewlett-Packard Company	Hardware Version: P/N AJ558-2102A; Firmware Version: Loader Version 0.67, PSMCU Version 2.13
2453	09/30/2015	Panorama M-100	Palo Alto Networks	Hardware Versions: P/Ns 910-000030 Version 00D, 910-000092 Version 00D, FIPS Kit P/N 920-000140 Version 00A; Firmware Version: 6.1.3
2454	09/30/2015	LogRhythm FIPS Object Module	LogRhythm	Software Version: 6.3.4