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

December 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 D Cooper

Dated: 1/4/2018

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 04/01/2018

Director, Architecture and Technology Assurance
Communications Security Establishment

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
3070	12/01/2017	Red Hat Enterprise Linux NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: 5.0
3071	12/01/2017	OmniSwitch AOS 6.7.1.R04 Cryptographic Module	Alcatel-Lucent Enterprise USA Inc.	Software Version: AOS 6.7.1.R04
3072	12/04/2017	NetApp CryptoMod	NetApp, Inc.	Software Version: 2.0
3073	12/05/2017	VMware VMkernel Cryptographic Module	VMware, Inc.	Software Version: 1.0
3074	12/06/2017	ASTRO PDEG Motorola Advanced Crypto Engine (MACE)	Motorola Solutions, Inc.	Hardware Version: P/Ns 5185912Y01, 5185912Y03, 5185912Y05 and 5185912T05; Firmware Version: R02.05.00
3075	12/06/2017	Samsung Flash Memory Protector V1.2.1	Samsung Electronics Co., Ltd.	Software Version: 1.3.1; Hardware Version: 3.0
3076	12/07/2017	Symantec SymSSLf Cryptographic Module	Symantec Corporation	Software Version: 1.0.1
3077	12/11/2017	Blue Coat Secure Web Gateway Virtual Appliance	Symantec Corporation	Software Version: 6.7.2
3078	12/11/2017	TrustedKeep Encryption Module	Trusted Concepts, Inc.	Software Version: 1.8.3
3079	12/11/2017	Datrium FIPS Object Module	Datrium	Software Version: 2.0.9, 2.0.10, 2.0.11 or 2.0.12
3080	12/13/2017	CryptoComply™ | Java	SafeLogic Inc.	Software Version: 3.0.1
3081	12/13/2017	Acme Packet VME	Oracle Communications	Software Version: ECz 7.5.0
3082	12/18/2017	Symantec Java Cryptographic Module	Symantec Corporation	Software Version: 1.3
3083	12/19/2017	Red Hat Enterprise Linux Libreswan Cryptographic Module	Red Hat(R), Inc.	Software Version: 5.0
3084	12/19/2017	Orbit MCR and Orbit ECR	GE MDS LLC	Hardware Version: MCR Chassis v1.0, ECR Chassis v1.0; Component PNs: U91, L4E, L4A, L9C, L7A, 4G1, 4G2, 4G3, 4G4, 4G5, 4GP, E4S, E42, W51, 3G1, NNN (refer to Security Policy Tables 1 and 2 for valid combinations); Firmware Version: 5.0.7

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
3085	12/19/2017	Brocade® MLXe® Series Ethernet Routers	Brocade Communications Systems, Inc.	Hardware Version: {[BR-MLXE-8-MR2-M-AC (80-1007225-01), BR-MLXE-8-MR2-M-DC (80-1007226-01), BR-MLXE-16-MR2-M-AC (80-1006827-02), BR-MLXE-16-MR2-M-DC (80-1006828-02), BR-MLXE-32-MR2-M-AC (80-1007253-04), BR-MLXE-32-MR2-M-DC (80-1007254-05), BR-MLXE-4-MR2-X-AC (80-1006874-03), BR-MLXE-4-MR2-X-DC (80-1006875-03), BR-MLXE-32-MR2-X-AC (80-1007255-04), BR-MLXE-32-MR2-X-DC (80-1007256-05)] with Component P/Ns 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, 80-1008425-01, 80-1008424-01, 80-1003891-02, 80-1002983-01, 80-1008686-01, 80-1003971-01, 80-1003969-02, 80-1003972-01, 80-1003970-03, 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 (as described in Security Policy, Table 13)} with FIPS Kit XBR-000195; Firmware Version: Multi-Service IronWare R06.0.00aa
3086	12/21/2017	nToken	Thales e-Security Inc.	Hardware Version: nC2023E-000, Build Standard N; Firmware Version: 2.51.10-2 and 2.55.1-2
3087	12/22/2017	Motorola Solutions Cryptographic Firmware Module	Motorola Solutions, Inc.	Firmware Version: R01.01.02
3088	12/28/2017	QTI Cryptographic Module on Crypto 5 Core	Zebra Technologies Corporation	Software Version: 5.f4-64; Hardware Version: Snapdragon 650