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

April 2018

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 A Cooper

Dated: 3/5/2018

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Raja Patt

Dated: 03/05/2018

Director, Security Architecture and Risk Management
Communications Security Establishment

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3096	04/11/2018	Secure Kernel Code Integrity	Microsoft Corporation	Software Version: 10.0.15063
3162	04/04/2018	Network Security Platform Sensor NS9300 S	McAfee, LLC	Hardware Version: P/Ns IPS-NS9300 S Version 1.30; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.2
3163	04/04/2018	Network Security Platform Sensor NS9300P	McAfee, LLC	Hardware Version: P/Ns IPS-NS9300 P Version 1.30; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.2
3164	04/04/2018	IBM 4767 Cryptographic Coprocessor Security Module	IBM Corporation	Hardware Version: 4767-001, P/N: 00LU348 POST0 v0110 MB0 v0102 and 4767-002, P/N: 00LV498 POST0 v0123 MB0 v0121; Firmware Version: 5.3.19 P0130 M0130 P0130 F0D01 (E2157B6F)
3165	04/04/2018	Aruba 2930M, 3810M and 5400R zl2 Switch Series	Hewlett Packard Enterprise	Hardware Version: Aruba 2930M Switches (JL319A, JL320A, JL321A, JL322A, JL323A, and JL324A) [1] with Expansion Cards listed in Table 2 of the Security Policy, Aruba 3810M Switches (JL071A, JL072A, JL073A, JL074A, JL075A, and JL076A) [2] with Expansion Cards listed in Table 3 of the Security Policy, Aruba 5400R zl2 Switches (5406R zl2 J9821A and 5412R zl2 J9822A) [3] with Management card and Interface Cards listed in Table 4 of the Security Policy; Firmware Version: WC.16.04.0011 [1] and KB.16.04.0011 [2] or [3]
3166	04/05/2018	Network Security Platform Sensor NS7150, NS7250 and NS7350	McAfee LLC	Hardware Version: P/Ns IPS-NS7150 Version 0.60, IPS-NS7250 Version 0.60 and IPS-NS7350 Version 0.60; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.1
3167	04/10/2018	IBM(R) Corporation LTO Generation 7 Encrypting Tape Drive	IBM(R) Corporation	Hardware Version: 38L7082 EC Level M13286 [1], 38L7458 EC Level N99160 [2], 38L7095 EC Level M13287 [3], 38L7448 EC Level N99160 [4], 38L7654 EC Level M13447 [5], 38L7651 EC Level M13447 [6]; Firmware Version: LTO7_G986.fcp_fh_f.fmrz [1], LTO7_G986.fcp_hh_f.fmrz [2], LTO7_G986.sas_hh_f.fmrz [3], LTO7_G986.fcp_fh_f_OEMD.fmrz [4], LTO7_G986.fcp_hh_f_OEMD.fmrz [5], LTO7_G986.sas_hh_f_OEMD.fmrz [6]
3168	04/10/2018	Oracle Linux 7 Libreswan Cryptographic Module	Oracle Corporation	Software Version: R7-2.0.0
3169	04/11/2018	Oracle Linux 7 GnuTLS Cryptographic Module	Oracle Corporation	Software Version: R7-2.0.0
3170	04/12/2018	Oracle Linux 6 Libreswan Cryptographic Module	Oracle Corporation	Software Version: R6-1.0.0
3171	04/15/2018	Pragma Systems Cryptographic Module	Pragma Systems, Inc.	Software Version: 2.0
3172	04/16/2018	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module 6.2.4	RSA Security LLC	Software Version: 6.2.4
3173	04/17/2018	HPE BladeSystem c-Class Virtual Connect Firmware	Hewlett Packard Enterprise Development LP	Firmware Version: 4.65

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3174	04/20/2018	HPE BladeSystem c-Class Onboard Administrator Firmware	Hewlett Packard Enterprise Development LP	Firmware Version: 4.71
3175	04/23/2018	JCOP 3 SecID P60 CS (OSB)	NXP Semiconductors	Hardware Version: P6022y VB; Firmware Version: 19790400
3176	04/26/2018	Digi ConnectCore Security Module	Digi International	Software Version: 1.0
3177	05/02/2018	Blue Coat Reverse Proxy Virtual Appliance	Symantec Corporation	Software Version: 6.7.2
3178	04/27/2018	Tintri Cryptographic Module	Tintri, Inc.	Software Version: 1.0
3179	04/30/2018	F5(R) vCMP Cryptographic Module	F5 Networks	Firmware Version: 13.1.0
3180	04/30/2018	Wave Relay® Embedded Module	Persistent Systems, LLC	Hardware Version: P/N WR-5200, Version 4.0; Firmware Version: 19.3.1