FIPS 140-2 Consolidated Validation Certificate

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

The Canadian Centre for Cyber Security

June 2019

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, 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: 7/9/19

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: July 9, 2019

Manager, Product Assurance and Standards
Canadian Centre for Cyber Security

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3466	06/03/2019	Gemalto FIPS Object Module	Gemalto, a Thales Company	Software Version: 2.1.0
3468	06/04/2019	Infinidat Cryptographic Module	Infinidat, Ltd.	Hardware Version: Intel Xeon E5-2697; Firmware Version: 1.0.1
3469	06/07/2019	Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, Windows 10 for Surface Hub	Microsoft Corporation	Software Version: 10.0.10586.1176
3470	06/07/2019	Crestron Crypto Kernel for OpenSSL	Crestron Electronics, Inc.	Software Version: 1.0
3471	06/10/2019	Samsung SAS 12G TCG Enterprise SSC SEDs PM1643 Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILT15THMLA-000H9, MZILT7T6HMLA-000H9, MZILT3T8HALS-000H9, MZILT1T9HAJQ-000H9 and MZILT920HAHQ-000H9; Firmware Version: 3P00
3472	06/12/2019	Nutanix Cryptographic Module for OpenSSH Client	Nutanix, Inc.	Software Version: OpenSSH client RPM package 7.4p1-16.el7 and fipscheck RPM package 1.4.1-6.el7
3473	06/12/2019	Nutanix Cryptographic Module for OpenSSH Server	Nutanix, Inc.	Software Version: OpenSSH server RPM package 7.4p1-16.el7 and fipscheck RPM package 1.4.1-6.el7
3474	06/12/2019	Oracle Linux OpenSSL Cryptographic Module	Oracle Corporation	Software Version: R7-3.0.0 [1] and R7-4.0.0 [2]
3475	06/14/2019	Aviatrix Cryptographic Module	Aviatrix Systems Inc.	Software Version: 1.0
3476	06/24/2019	Aruba AP-204, AP-205 and AP-205H Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-204-F1 (HPE SKU JW163A), AP-205-F1 (HPE SKU JW165A) and AP-205H-F1 (HPE SKU JW167A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.2-FIPS
3477	06/25/2019	NetLib® Encryptionizer® Platform (NEP)	NetLib Security, Inc.	Software Version: 2018.1.1.0
3478	06/27/2019	WildFire WF-500	Palo Alto Networks	Hardware Version: 910-000097-00G; FIPS Kit P/N: 920-000145-00A; Firmware Version: 8.1.6
3479	06/27/2019	Palo Alto Networks VM-Series	Palo Alto Networks	Software Version: 8.1.3 and 8.1.6
3480	06/28/2019	Windows OS Loader	Microsoft Corporation	Software Version: 10.0.17134