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

December 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 A Cooper

Dated: 1/21/2020

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: January 15, 2020

Manager, ProductAssurance 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
3574	12/03/2019	Network Security Platform Sensor NS3100, NS3200, NS5100 and NS5200	McAfee, LLC	Hardware Version: P/Ns IPS-NS3100 Version 1.00, IPS-NS3200 Version 1.00, IPS-NS5100 Version 1.00 and IPS-NS5200 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.100
3575	12/04/2019	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: 9.1.17.100
3576	12/04/2019	Network Security Platform Sensor NS7100, NS7200 and NS7300	McAfee, LLC	Hardware Version: P/Ns IPS-NS7100 Version 1.00, IPS-NS7200 Version 1.00 and IPS-NS7300 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.100
3577	12/04/2019	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: 9.1.17.100
3578	12/04/2019	Extreme Networks FIPS Object Module	Extreme Networks	Software Version: 2.0.16i or 2.0.16m
3579	12/09/2019	Samsung SAS 12G TCG Enterprise SSC SEDs PM1643/PM1645 Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILT800HAHQ-000C9 [3], MZILT960HAHQ-000C9 [1], MZILT1T6HAJQ-000C9 [3], MZILT1T9HAJQ-000C9 [1], MZILT3T2HALS-000C9 [3], MZILT3T8HALS-000C9 [1], MZILT7T6HMLA-000C9 [2], MZILT15THMLA-000C9 [2] and MZILT30THMLA-000C9 [2]; Firmware Version: EXF7 [1], EXV7 [2] and EZF7 [3]
3580	12/09/2019	Network Security Platform Sensor NS9100 and NS9200	McAfee, LLC	Hardware Version: P/Ns IPS-NS9100 Version 1.00 and IPS-NS9200 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.100
3581	12/11/2019	Accellion Cryptographic Module	Accellion, Inc.	Software Version: 1.0
3582	12/12/2019	Oracle Linux 7 OpenSSH Client Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
3583	12/13/2019	Samsung BoringSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.3
3584	12/17/2019	HPE SimpliVity OmniStack Crypto Library	Hewlett Packard Enterprise Development LP	Software Version: 2.1
3585	12/17/2019	BC-FJA (Bouncy Castle FIPS Java API)	Legion of the Bouncy Castle Inc.	Software Version: 1.0.0
3586	12/20/2019	Aruba AP-203R, AP-203RP, and AP-303H Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-203R-USF1 (HPE SKU JY715A), AP-203R-RWF1 (HPE SKU JY713A), AP-203RP-USF1 (HPE SKU JY723A), AP-203RP-RWF1 (HPE SKU JY721A), AP-303H-USF1 (HPE SKU JY681A) and AP-303H-RWF1 (HPE SKU JY679A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.2.2.5-FIPS

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3587	12/30/2019	X4i Postal Security Device (PSD)	Pitney Bowes, Inc.	Hardware Version: MAX32590 Secure Microcontroller Revision B4; Firmware Version: PB Bootloader Version 00.00.0016, PSD Application Version 21.06.0013 [1] or 21.07.000A [2], and Device Abstraction Layer (DAL) Version 01.02.0018 [1] or 01.02.0024 [2]