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

October 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: 11/13/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: November 13, 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
3541	10/01/2019	Nutanix Cryptographic Module for BoringSSL	Nutanix	Software Version: 66005f41fbc3529ffe8d007708756720529da20d
3542	10/02/2019	VMware's VPN Crypto Module	VMware, Inc.	Software Version: 1.0
3543	10/02/2019	Netskope Cryptographic Security Module	Netskope Inc.	Software Version: 2.0.16
3544	10/03/2019	Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.15063.728
3545	10/04/2019	Fortanix SDKMS Appliance	Fortanix, Inc.	Hardware Version: FX2200; Firmware Version: 2.2.652
3546	10/08/2019	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.0
3547	10/08/2019	Samsung Flash Memory Protector V1.5	Samsung Electronics Co., Ltd.	Software Version: 1.5; Hardware Version: 5.0
3548	10/09/2019	RF-7800W Integrated Radio/PA	Harris Corporation	Hardware Version: RF-7800W-RP50x and RF-7800W-RP47x; Firmware Version: 6.00
3549	10/10/2019	Qualcomm(R) Secure Processing Unit (SPU)	Qualcomm Technologies, Inc.	Hardware Version: 3.1; Firmware Version: spss.a1.1.2_00078
3550	10/18/2019	VMware's OpenSSL FIPS Object Module	VMware, Inc.	Software Version: 2.0.20-vmw
3551	10/21/2019	Aruba AP-304, AP-305, AP-314, AP-315, AP-334, AP-335, AP-365, and AP-367 Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-304-F1 (HPE SKU JX937A), AP-305-F1 (HPE SKU JX938A), AP-314-F1 (HPE SKU JW796A), AP-315-F1 (HPE SKU JW798A), AP-334-F1 (HPE SKU JW800A), AP-335-F1 (HPE SKU JW802A), AP-365-F1 (HPE SKU JX969A) and AP-367-F1 (HPE SKU JX976A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.2.2.5-FIPS
3552	10/21/2019	Aruba 7XXX Series Controllers with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [Aruba 7005-RWF1 (HPE SKU JW635A), Aruba 7005-USF1 (HPE SKU JW636A), Aruba 7008-RWF1 (HPE SKU JX931A), Aruba 7008-USF1 (HPE SKU JX932A), Aruba 7010-RWF1 (HPE SKU JW702A), Aruba 7010-USF1 (HPE SKU JW703A), Aruba 7024-RWF1 (HPE SKU JW706A), Aruba 7024-USF1 (HPE SKU JW707A), Aruba 7030-RWF1 (HPE SKU JW710A), Aruba 7030-USF1 (HPE SKU JW711A), Aruba 7205-RWF1 (HPE SKU JW739A), Aruba 7205-USF1 (HPE SKU JW740A), Aruba 7210-RWF1 (HPE SKU JW745A), Aruba 7210-USF1 (HPE SKU JW746A), Aruba 7220-RWF1 (HPE SKU JW753A), Aruba 7220-USF1 (HPE SKU JW754A), Aruba 7240-RWF1 (HPE SKU JW761A), Aruba 7240XM-RWF1 (HPE SKU JW829A), Aruba 7240-USF1 (HPE SKU JW762A), Aruba 7240XM-USF1 (HPE SKU JW830A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.2.2.5-FIPS
3553	10/23/2019	Amazon Linux 2 OpenSSL Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3554	10/23/2019	Cisco Systems NSS Module	Cisco Systems, Inc.	Software Version: 3.36
3555	10/23/2019	IBM(R) z/OS(R) Version 2 Release 3 ICSF PKCS #11 Cryptographic Module	IBM Corporation	Software Version: HCR77C0 with APAR OA56129; Hardware Version: COP chips integrated within processor unit [1], COP chips integrated within processor unit and P/N 00LV498 [2] and COP chips integrated within processor unit and P/N 01PP167 [3]; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 32L [1], Feature 3863 (aka FC3863) with System Driver Level 32L and CCA 5.3.20z [2] and Feature 3863 (aka FC3863) with System Driver Level 32L and CCA 6.0.8z [3]
3556	10/24/2019	CRATON2/SECTON embedded V2X HSM	Autotalks Ltd.	Hardware Version: P/N ATK66610, Version 2.1.2; Firmware Version: 2.1.2
3557	10/25/2019	IBM(R) z/OS(R) Version 2 Release 3 System SSL Cryptographic Module	IBM Corporation	Software Version: HCPT430/JCPT431 with APAR OA57026; Hardware Version: COP chips integrated within processor unit; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 32L
3558	10/28/2019	Aviat Networks Eclipse Cryptographic Module	Aviat Networks, Inc.	Hardware Version: INUe 2RU Chassis (P/N EXE-002), Fan Card (P/N EXF-101), Node Controller Card (P/N EXN-004 with FPGA_NCCV2_E1_DS1_004.bit and FPGA_NCCV2_STM1_006.bit), FIPS Installation Kit (P/N 179-530153-001 or 179-530153-002), Replacement Seals (P/N 007-600331-001), at least one of: [RAC 6X (P/N EXR-600-001 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 6XE (P/N EXR-600-002 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 60 (P/N EXR-660-001 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 60E (P/N EXR-660-002 with FPGA_RAC6X_PDH_ACM-14.19.52.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 70 (P/N EXR-700-001 with FPGA_RAC7X_R2-2.18.9.bit) or RAC 7X (P/N EXR-770-001 with FPGA_RAC7X_R2-2.18.9.bit)] and all remaining slots filled by excluded components as specified in the Security Policy.; Firmware Version: 08.04.91 with Bootloader version 1.0.36