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

September 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 J Cooper

Dated: 10/3/2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 03/10/2017

Director, Architecture and Technology Assurance
Communications Security Establishment

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

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
3009	09/05/2017	AWS Key Management Service HSM	Amazon Web Services, Inc.	Hardware Version: 2.0; Firmware Version: 1.3.6
3010	09/06/2017	Attivo Cryptographic Provider	Attivo Networks Inc.	Software Version: 1.0
3011	09/07/2017	Unified Crypto Module	Comtech EF Data Corporation	Hardware Version: PL-0000235-2; Firmware Version: 2.2.4
3012	09/08/2017	Red Hat Enterprise Linux GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: 5.0
3013	09/13/2017	X-Wall MX+	Enova Technology Corporation	Hardware Version: xF; Firmware Version: mr17.03.27.220.Enova
3014	09/13/2017	X-Wall MX+	Enova Technology Corporation	Hardware Version: xN; Firmware Version: mr17.03.27.220.Enova
3015	09/15/2017	iPASOLINK AES MODEM Card (MODEM-AEH)	NEC Corporation	Hardware Version: NWA-086220-004
3016	09/15/2017	Red Hat Enterprise Linux OpenSSL Cryptographic Module	Red Hat(R), Inc.	Software Version: 5.0
3017	09/20/2017	Oracle Linux OpenSSL Cryptographic Module	Oracle Corporation	Software Version: R6-1.0.0[1] and R7-2.0.0[2]
3018	09/21/2017	Hewlett Packard Enterprise SSL crypto module	Hewlett Packard Enterprise	Software Version: 2.1
3019	09/21/2017	IBM(R) z/OS(R) Version 2 Release 2 ICSF PKCS #11 Cryptographic Module	IBM Corporation	Software Version: OA52336; Hardware Version: COP chips integrated within processor unit [1] and P/N 00LV487 [2]; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 27I [1] and CCA 5.2.27z RC30 [2]
3020	09/21/2017	INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit	INTEGRITY Security Services	Software Version: 3.0.0
3021	09/22/2017	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 6.5.1-FIPS
3022	09/22/2017	Aruba AP-214, AP-215, AP-274, AP-275, AP-277 and AP-228 Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-214-F1 (HPE SKU JW169A), AP-215-F1 (HPE SKU JW171A), AP-274-F1 (HPE SKU JW177A), AP-275-F1 (HPE SKU JW179A), AP-277-F1 (HPE SKU JW181A) and AP-228-F1 (HPE SKU JW183A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 6.5.1-FIPS
3023	09/22/2017	Aruba RAP-108 and RAP-109 Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [RAP-108-F1 (HPE SKU JW268A), RAP-108-USF1 (HPE SKU JW269A), RAP-109-F1 (HPE SKU JW274A) and RAP-109-USF1 (HPE SKU JW275A)] with FIPS kit 4011570-01; Firmware Version: ArubaOS 6.5.1-FIPS
3024	09/22/2017	Aruba AP-224 and AP-225 Wireless Access Points	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-224-F1 (HPE SKU JW173A) and AP-225-F1 (HPE SKU JW175A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 6.5.1-FIPS

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3025	09/22/2017	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 7010-RWF1 (HPE SKU JW702A), Aruba 7010-USF1 (HPE SKU JW703A), Aruba 7024-RWF1 (HPE SKU JW706A0), Aruba 7024-USF1 (HPE SKU JW707A), Aruba 7030-RWF1 (HPE SKU JW710A), Aruba 7030-USF1 (HPE SKU JW711A), Aruba 7205-RWF1 (HPE SKU JW739A) and Aruba 7205-USF1 (HPE SKU JW740A)} with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 6.5.1-FIPS
3026	09/22/2017	Aruba 7200 Series Controllers with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Hardware Version: {Aruba 7210-F1 (HPE SKU JW745A), Aruba 7210-USF1 (HPE SKU JW746A), Aruba 7220-F1 (HPE SKU JW753A), Aruba 7220-USF1 (HPE SKU JW754A), Aruba 7240-F1 (HPE SKU JW761A), Aruba 7240XM-RWF1 (HPE SKU JW829A), Aruba 7240-USF1 (HPE SKU JW762A) and Aruba 7240XM-USF1 (HPE SKU JW830A)} with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 6.5.1-FIPS
3027	09/25/2017	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.0
3028	09/27/2017	Oracle Linux 7 OpenSSH Server Cryptographic Module	Oracle Corporation	Software Version: R7-2.0.0
3029	09/27/2017	BlackVault HSM	Engage Communication, Inc.	Hardware Version: 007-BVES-01; Firmware Version: 7.0.10
3030	09/28/2017	Oracle Linux 6 OpenSSH Client Cryptographic Module	Oracle Corporation	Software Version: R6-1.0.0
3031	09/29/2017	Oracle Linux 6 OpenSSH Server Cryptographic Module	Oracle Corporation	Software Version: R6-1.0.0
3032	09/29/2017	Oracle Linux 7 OpenSSH Client Cryptographic Module	Oracle Corporation	Software Version: R7-2.0.0