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 2023

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: TIMOTHY HALL Digitally signed by TIMOTHY HALL Date: 2023.11.06 10:43:54 -05'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall Digitally signed by King, Lyall DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall" Reason: I am approving this document Location: Date: 2023.11.03 10:43:03-04'00' Foxit PDF Editor Version: 12.1.2

Dated: _____

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

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

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4621	10/02/2023	Axis Cryptographic Module	Axis Communications AB	Software Version: 3.0.8
4622	10/02/2023	NPCT7xx TPM 2.0 rev 1.38	Nuvoton Technology Corporation	Hardware Version: LAG019 in TSSOP28 Package, LAG019 in QFN32 Package, and LAG019 in UQFN16 Package; Firmware Version: 7.2.2.0
4623	10/03/2023	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 8.10.0.2-FIPS
4624	10/03/2023	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-USF1 (HPE SKU JX937A), AP-305-USF1 (HPE SKU JX938A), AP-314-USF1 (HPE SKU JW796A), AP-315-USF1 (HPE SKU JW798A), AP-334-USF1 (HPE SKU JW800A), AP-335-USF1 (HPE SKU JW802A), AP-365-USF1 (HPE SKU JX969A) and AP-367-USF1 (HPE SKU JX976A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.10.0.2-FIPS
4625	10/04/2023	Juniper Networks SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 Services Gateway	Juniper Networks, Inc	Hardware Version: SRX345, SRX345-DUAL-AC, SRX380, SRX1500 SYS-JB-AC and SRX1500 SYS-JB-DC with JNPR-FIPS-TAMPER-LBLS; Firmware Version: Junos OS 20.2R1
4626	10/04/2023	AMD Ryzen PRO 6000 Series PSP Cryptographic CoProcessor	Advanced Micro Devices (AMD)	Hardware Version: bc0d0253FIPS002; Firmware Version: bc0d0253FIPS002
4627	10/04/2023	Allegro Cryptographic Engine	Allegro Software Development Corporation	Software Version: 6.3.3
4628	10/05/2023	Citrix FIPS Cryptographic Module	Citrix Systems, Inc.	Software Version: 1.0, 1.0.1 and 1.0.2; Hardware Version: ARM v8-A, ARM v7-A, Intel Core i7 4th Generation, Intel Core i7 6th Generation, Intel Core i7 8th Generation, Intel Xeon 56xx series, Intel Xeon E5-24xx v2 series, Intel Xeon E5-26xx v2 series, Intel Xeon E5-26xx v3 series and Intel Xeon E5-26xx v4 series
4629	10/05/2023	Aruba AP-504, AP-505, AP-514, AP-515, AP-534, AP-535 and AP-555 Wireless Access Points with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-504-USF1 (HPE SKU R2H34A), AP-505-USF1 (HPE SKU R2H39A), AP-514-USF1 (HPE SKU Q9H68A), AP-515-USF1 (HPE SKU Q9H73A), AP-534-USF1 (HPE SKU JZ342A), AP-535-USF1 (HPE SKU JZ347A), AP-555-USF1 (HPE SKU JZ367A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.10.0.2-FIPS
4630	10/05/2023	Aruba Mobility Controller Virtual Appliances with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Firmware Version: ArubaOS 8.10.0.2-FIPS
4631	10/06/2023	AWS-LC Cryptographic Module	Amazon Web Services Inc.	Software Version: AWS-LC FIPS 1.0.2
4632	10/09/2023	Datastax BC-FJA (Bouncy Castle FIPS Java API)	DataStax, Inc.	Software Version: 1.0.2.3

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4633	10/11/2023	ASI-HSM AHX5 KNET Cryptographic Module	KRYPTUS S.A.	Hardware Version: 1.0.1; Firmware Version: 1.0.1
4634	10/11/2023	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 8.10.0.2-FIPS
4635	10/11/2023	Avaya G450/G430 FIPS 140-2 Cryptographic Module	Avaya, Inc.	Hardware Version: P/Ns 700506955, 700506955 with 700501368, 700512173 and 700512173 with 700503274; Firmware Version: 41.34.5
4636	10/12/2023	SBC 5400 Session Border Controller	Ribbon Communications, Inc.	Hardware Version: SBC 5400 with ASPEED AST2400 and FIPS Kit 550-06508; Firmware Version: R7.2.1S0
4637	10/12/2023	Aruba Virtual and Hardware Mobility Master Appliances with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Firmware Version: ArubaOS 8.10.0.2-FIPS
4638	10/18/2023	Cisco ISR 1000 Series Routers without MACSEC	Cisco Systems, Inc.	Hardware Version: ISR1101 and ISR1111; Firmware Version: Cisco IOS-XE 16.12
4639	10/23/2023	Kemp LoadMaster FIPS Object Module	Progress Software Corporation	Software Version: v1.0
4640	10/23/2023	Secure Kernel Code Integrity	Microsoft Corporation	Software Version: 10.0.17763.10021 and 10.0.17763.10127
4641	10/25/2023	SonicWall Network Security Manager Appliance	SonicWall, Inc.	Firmware Version: 2.3
4642	10/25/2023	Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20220323
4643	10/25/2023	Cisco ASR 1000 Series Routers without MACSEC	Cisco Systems, Inc.	Hardware Version: ASR1002-X, [ASR1004 and ASR1006 with components ASR-1000-RP2, ASR1000-ESP20 and ASR1000-ESP40]; Firmware Version: Cisco IOS-XE 16.12

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4644	10/25/2023	Cisco ASR 1000 Series Routers with MACSEC	Cisco Systems, Inc.	Hardware Version: ASR1001-HX, ASR1002-HX, [[ASR1006-X with RP2, RP3, ESP40, ESP100, [ASR1000-MIP100 with EPA-10X10GE and EPA-1X40GE QSFP+]] and [[ASR-1009-X with RP2, RP3, ESP40, ESP100, ESP200, [ASR1000-MIP100 with EPA-10X10GE and EPA-1X40GE QSFP+]]; Firmware Version: Cisco IOS-XE 16.12
4645	10/25/2023	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module 6.2.5	Dell Inc., BSAFE Product Team	Software Version: 6.2.5
4646	10/25/2023	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module 6.2.5	Dell Inc., BSAFE Product Team	Software Version: 6.2.5
4647	10/26/2023	Qualcomm(R) Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.6.2[1], 5.6.1[2] and 5.6.5[3]
4648	10/26/2023	Cryptographic Module for Intel® Platforms' Security Engine Chipset	Intel Corporation	Hardware Version: 2.0; Firmware Version: 3.1
4649	10/27/2023	Maxar AEDS	Maxar Technologies	Hardware Version: Revision 1; Firmware Version: 1.0.6.1558.2958