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

February 2021

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: Gavin O'Brien

Dated: 03/02/2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 02/03/2021

Director, Risk Mitigation Programs
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
3805	02/01/2021	Key Variable Loader (KVL) 4000 PIKE2	Motorola Solutions, Inc.	Hardware Version: P/N 51009397004; Firmware Version: R02.07.30 with or without AES128 R01.01.00, AES256 R01.01.00, and/or ADP/CFX-256/DES-XL/DES/DVI-XL/DVP-XL/Localized Capable R01.00.00
3806	02/02/2021	Summit Linux FIPS Core Crypto Module	Laird Connectivity	Software Version: 7.0; Hardware Version: ATSAMA5D31 and ATSAMA5D36
3807	02/02/2021	Cisco ASA and ISA Cryptographic Modules	Cisco Systems, Inc.	Hardware Version: ASA 5506-X[1][2], ASA 5506H-X[1][2], ASA 5506W-X[1][2], ASA 5508-X[1][3], ASA 5516-X[1][4], ASA 5525-X[1], ASA 5545-X[1], ASA 5555-X[1], ISA 3000-4C[1] and ISA 3000-2C2F[1] with [AIR-AP-FIPSKIT=][1], [ASA5506-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3] and [ASA5516-FIPS-KIT=][4]; Firmware Version: 9.12
3808	02/02/2021	Ultrastar® DC SS540 TCG Enterprise SSD	Western Digital Corporation	Hardware Version: P/Ns WUSTM3240BSS205 [1, 2], WUSTM3280BSS205 [1, 2], WUSTM3216BSS205 [1, 2], WUSTM3232BSS205 [1, 2], WUSTR6480BSS205 [1, 2, 3, 4], WUSTR6416BSS205 [1, 2, 3, 4], WUSTR6432BSS205 [1, 2, 3, 4], WUSTR6464BSS205 [1, 2, 4], WUSTVA196BSS205 [1, 2, 4], WUSTVA119BSS205 [1, 2, 4], WUSTVA138BSS205 [1, 2, 3, 4], WUSTVA176BSS205 [1, 2, 3, 4] and WUSTVA1A1BSS205 [1, 2, 3, 4]; Firmware Version: R088 [1], R104 [2], R109 [3] and R10A [4]
3809	02/03/2021	Cisco Firepower Next-Generation IPS Virtual (NGIPSv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.4
3810	02/03/2021	HPE XP8 Encrypt Backend 4pk NVMe I/O Mod (eDKBN)	Hewlett Packard Enterprise Company	Hardware Version: P/N: 3292549-A; Version: A; Firmware Version: 90-00-01
3811	02/05/2021	Apple Secure Key Store Cryptographic Module, v10.0	Apple Inc.	Hardware Version: 1.2[1], 2.0[2]; Firmware Version: SEPOS
3812	02/05/2021	Palo Alto Networks Cortex XSOAR Module	Palo Alto Networks	Software Version: 1.0
3813	02/08/2021	Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20190816
3814	02/08/2021	FortiOS 6.0 and 6.2	Fortinet, Inc.	Firmware Version: FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548
3815	02/09/2021	Cisco ISR 4000 Series Routers with MACSEC	Cisco Systems, Inc.	Hardware Version: ISR 4321, ISR 4331, ISR 4351 and ISR 4451 with NIM-2GE-CU-SFP; Firmware Version: Cisco IOS XE 16.9
3816	02/09/2021	Junos Space Network Management Platform, with or without Network Director and with or without Security Director in JA2500	Juniper Networks, Inc.	Hardware Version: JA2500; Firmware Version: Junos Space 19.1R1_FIPS, Network-Director.3.6R3.15 and Security-Director-19.1R1.23

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3817	02/09/2021	Cisco Network Convergence System 1001 Cryptographic Module	Cisco Systems, Inc.	Hardware Version: NCS1001-K9=, NCS1K-CNTLR2, NCS1K-EDFA, NCS1K-PSM and NCS1K-OTDR with FIPS Kit (AIR-AP-FIPSKIT=); Firmware Version: IOS XR 7.0.1
3818	02/09/2021	Cisco Network Convergence System 1004 Cryptographic Module	Cisco Systems, Inc.	Hardware Version: NCS1004=, NCS1K4-CNTLR-K9=, NCS1K4-1.2T-K9 and NCS1K4-1.2T-L-K9 with FIPS Kit (AIR-AP-FIPSKIT=); Firmware Version: IOS XR 7.0.1
3819	02/17/2021	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module 6.2.5	RSA Security LLC	Software Version: 6.2.5
3820	02/17/2021	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module 6.2.5	RSA Security LLC	Software Version: 6.2.5
3821	02/23/2021	Cisco Firepower Threat Defense on 4K/9K Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR4110, FPR4115, FPR4120, FPR4125, FPR4140, FPR4145, FPR4150, FPR9K-SM-24, FPR9K-SM-36, FPR9K-SM-40, FPR9K-SM-44, FPR9K-SM-48 and FPR9K-SM-56; Firmware Version: 6.4
3822	02/23/2021	Juniper Networks EX4300-48MP Ethernet Switch	Juniper Networks, Inc.	Hardware Version: EX4300-48MP; Firmware Version: Junos OS 19.4R1
3823	02/23/2021	Cisco ASA and ISA Firepower Threat Defense Cryptographic Modules	Cisco Systems, Inc.	Hardware Version: ASA 5508-X[1][2], ASA 5516-X[1][3], ISA 3000-4C[1] and ISA 3000-2C2F[1] with [AIR-AP-FIPSKIT=][1], [ASA5508-FIPS-KIT=][2] and [ASA5516-FIPS-KIT=][3]; Firmware Version: 6.4
3825	02/24/2021	VMware's Linux Cryptographic Module	VMware, Inc.	Software Version: v3.0
3826	02/24/2021	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 8.6.0.7-FIPS
3827	02/24/2021	CMS-5000	QSC, LLC	Hardware Version: AP-000128-01 Rev J; Firmware Version: 1.0.01391
3828	02/25/2021	Honeywell Mobility Edge™ BoringCrypto	Honeywell International Inc.	Software Version: 2.0
3829	02/26/2021	CryptoComply for HSM	SafeLogic Inc.	Hardware Version: Se-Series Gen2 Versions 5.01.2.0 and 5.01.4.0; Firmware Version: Firmware Package Version 5.0.10.1
3830	02/26/2021	X4i Hardware Security Module (HSM)	Pitney Bowes, Inc.	Hardware Version: MAX32590 Secure Microcontroller Revision B4; Firmware Version: PB Bootloader Version 00.00.0016, HSM Application Version 21.02.000F [1] or 21.03.0001 [2], and Device Abstraction Layer (DAL) Version 01.02.0018 [1] or 01.02.0024 [2]