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

November 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: TIMOTHY HALL Digitally signed by TIMOTHY HALL Date: 2021.12.08 12:43:43 -05'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: December 08 2021

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
4064	11/01/2021	µMACE	Motorola Solutions, Inc.	Hardware Version: P/N 51009730001, Rev 0x0001; Firmware Version: R03.03.09 with or without AES128 R01.00.01, AES256 R01.00.03, and/or ADP/DES-XL/DES-OFB/DES-ECB/DES-CBC/DVI-XL/DVP-XL/Localized Capable R01.00.00
4065	11/02/2021	Thales Alenia Space cryptographic module for Microsemi RTAX FPGA	Thales Alenia Space	Hardware Version: RTAX2000S FPGA; 28C010T EEPROM; Firmware Version: 3.32.00; 3.32.04
4066	11/02/2021	Gigamon's BC-FJA (Bouncy Castle FIPS Java API)	Gigamon Inc.	Software Version: 1.0.2.1
4067	11/04/2021	Aruba AP-318, AP-344, AP-345, AP-374, AP-375, AP-377 and AP-387 Outdoor Access Points with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [AP-318-USF1 (HPE SKU JZ158A), AP-318-RWF1 (HPE SKU JZ157A), AP-344-USF1 (HPE SKU JZ024A), AP-344-RWF1 (HPE SKU JZ022A), AP-345-USF1 (HPE SKU JZ034A), AP-345-RWF1 (HPE SKU JZ032A), AP-374-USF1 (HPE SKU JZ168A), AP-374-RWF1 (HPE SKU JZ167A), AP-375-USF1 (HPE SKU JZ178A), AP-375-RWF1 (HPE SKU JZ177A), AP-377-USF1 (HPE SKU JZ188A), AP-377-RWF1 (HPE SKU JZ187A), AP-387-USF1 (HPE SKU R0K14A), AP-387-RWF1 (HPE SKU R0K13A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.6.0.7-FIPS
4068	11/09/2021	Unisys Linux Kernel Cryptographic API Module	Unisys Corporation	Software Version: 2.0
4069	11/15/2021	SUSE Linux Enterprise Kernel Crypto API Cryptographic Module	SUSE, LLC	Software Version: 2.1
4070	11/15/2021	SUSE Linux Enterprise OpenSSL Cryptographic Module	SUSE, LLC	Software Version: 3.1
4071	11/16/2021	REDCOM Crypto Module	REDCOM Laboratories, Inc.	Software Version: 2.2
4072	11/17/2021	FortiGate-600D/1200D/1500D/3000D/3700D and FortiGate-5001D with FortiGate-5144C Chassis	Fortinet, Inc.	Hardware Version: FortiGate-600D (C1AE11), FortiGate-1200D (C1AC57), FortiGate-1500D (C1AA64), FortiGate-3000D (C1AC63), FortiGate-3700D (C1AA92), FortiGate-5001D (C1AA92), FortiGate-5144C (C1AB98), Blank Filler Panel - Front (P16708-01) and Blank Filler Panel - Rear (P16710-01) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548
4073	11/17/2021	FortiGate-VM	Fortinet, Inc.	Software Version: FortiGate-VM 6.2, build 5611
4074	11/18/2021	FireEye HX Series: HX4402, HX4502, HX4502D	FireEye, Inc.	Hardware Version: HX4402, HX4502, HX4502D; Firmware Version: 5.0.4
4075	11/18/2021	Fortanix SDKMS Appliance (FX2200, Version 3.10.16)	Fortanix, Inc.	Hardware Version: FX2200; Firmware Version: 3.10.16

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4076	11/22/2021	Hitachi Virtual Storage Platform (VSP) Encryption Board for NVMe	Hitachi, Ltd.	Hardware Version: P/N:VSPEBN-001 Version: 001; Firmware Version: FPGA Main Firmware Ver: ED000B2E; FPGA Configuration data Ver: ED000002_19112100; FPGA bootloader Firmware Ver: 00000003
4077	11/27/2021	Samsung Flash Memory Protector V3.0	Samsung Electronics Co., Ltd.	Software Version: 3.0; Hardware Version: FX8_4.10
4078	11/29/2021	Qualcomm(R) Trusted Execution Environment (TEE) Software Cryptographic Library	Qualcomm Technologies, Inc.	Software Version: 5.11-00043.1; Hardware Version: Snapdragon 888 5G Mobile Platform
4079	11/29/2021	IBM 4769-001 Cryptographic Coprocessor Security Module	IBM Corporation	Hardware Version: PNs 4769-001: PN 02WN652-N37880 POST0 v9662 MB0 v6096 (Standard Power) and 4769-001: PN 02WN654-N37880 POST0 v9662 MB0 v6096 (Low Power); Firmware Version: 7.0.46z P1591 M1591 P5625 F0701 (2B5F92F3)
4080	11/30/2021	Johnson Encryption Machine 2 (JEM2)	EF Johnson Technologies	Hardware Version: P/Ns R035-3900-180-00 and R035-3900-280-01; Firmware Version: 4.2
4081	11/30/2021	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 21.07.000F, and Device Abstraction Layer (DAL) Version 01.02.0027
4082	11/30/2021	Cisco 8200 Series Routers	Cisco Systems, Inc.	Hardware Version: 8201-SYS and 8202-SYS; Firmware Version: IOS-XR 7.0
4083	11/30/2021	DINAMO Pocket Hardware Security Module	DINAMO Networks, Inc.	Hardware Version: DINAMO Pocket; Firmware Version: 5.0.8.0
4084	11/30/2021	Ultrastar® DC HC550 TCG Enterprise HDD	Western Digital Corporation	Hardware Version: WUH721816AL5205, WUH721818AL5205, WUH721816AL4205 and WUH721818AL4205; Firmware Version: R290, R650 and UM05
4085	11/30/2021	GSP3000 Hardware Security Module	Futurex	Hardware Version: P/Ns 9800-2079 Rev7, Rev8, Rev8C, Rev8D, Rev9A.A, Rev9B.A, Rev9C.A, Rev9D.A, Rev9A.B, Rev9B.B, Rev9C.B or Rev9D.B; Firmware Version: 7.0.0.3
4086	11/30/2021	EXP1000 Hardware Security Module	Futurex	Hardware Version: P/Ns 9850-0365 Rev10, 9800-2082 Rev 10, 9800-2082 Rev 10A, 9800-2082 Rev 10B, 9800-2082 Rev 10C, 9800-2082 Rev 10D, 9800-2082 Rev 10E, 9800-2082 Rev 11 and 9800-2082 Rev 11A; Firmware Version: 7.0.0.3