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

December 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: 2022.01.06 08:46:24 -05'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: January 5 2022

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
4087	12/01/2021	Aruba 7280 Series Controller with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise Company	Hardware Version: [Aruba 7280-USF1 (HPE SKU JX914A) and Aruba 7280-RWF1 (HPE SKU JX915A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.6.0.7-FIPS
4088	12/02/2021	Poly Crypto Module for MobileOS	Plantronics, Inc.	Software Version: 1.0
4089	12/02/2021	Virtual System Administrator (VSA) Cryptographic Module	Kaseya US LLC	Software Version: 2.2
4090	12/02/2021	Thales Luna K7 Cryptographic Module	Thales	Hardware Version: 808-000048-002, 808-000066-001and 808-000073-001; Firmware Version: 7.7.0 or 7.7.1 with Boot Loader versions 1.1.1, 1.1.2 or 1.1.4
4091	12/03/2021	Provizio Crypto Module	Bruin Biometrics LLC	Software Version: 6.3
4092	12/05/2021	Samsung Flash Memory Protector V3.0.1	Samsung Electronics Co., Ltd.	Software Version: 3.0.1; Hardware Version: HX4_v3.1
4093	12/06/2021	Qualcomm(R) Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.6.0
4094	12/06/2021	Riverbed Cryptographic Module v1.1	Riverbed	Software Version: 1.1
4095	12/06/2021	Tigera Cryptographic Module	Tigera, Inc.	Software Version: ae223d6138807a13006342edfeef32e813246b39
4096	12/06/2021	InformaCast Java Crypto Library	Singlewire Software	Software Version: 3.0.1
4097	12/11/2021	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.2
4098	12/12/2021	Citrix ADC VPX	Citrix Systems, Inc.	Software Version: 12.1.55.180
4099	12/13/2021	Qualcomm(R) Pseudo Random Number Generator	Spectralink Corporation	Hardware Version: 2.3.1
4100	12/13/2021	Sophos Cryptographic Module	Sophos Limited	Software Version: 1.0
4101	12/13/2021	CERDEC Cryptographic Module 1.0.2	US Army CERDEC	Hardware Version: M2S050TS-1FGG896 and 1.0PL; Firmware Version: FreeRTOS 7.0.1 and Crypto Engine 1.0.2
4102	12/13/2021	Poly Crypto Module for Java	Plantronics, Inc.	Software Version: 3.0.1
4103	12/13/2021	Cloudera Cryptographic Module for Java	Cloudera, Inc.	Software Version: 3.0.1
4104	12/13/2021	CAPKI for Server	Broadcom	Software Version: 2.2
4105	12/13/2021	CTERA Crypto Module (Java)	CTERA Networks Ltd.	Software Version: 3.0.1
4106	12/13/2021	Cloudera Cryptographic Module for OpenSSL	Cloudera, Inc.	Software Version: 2.2
4107	12/14/2021	VAST Data FIPS Object Module for OpenSSL	VAST Data	Software Version: 1.0
4108	12/15/2021	Dell OpenSSL Cryptographic Library	Dell, Inc.	Software Version: 2.6

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4109	12/16/2021	Purity Encryption Module	Pure Storage, Inc.	Software Version: 1.3; Hardware Version: Intel Xeon E5-2698 v4, Intel Xeon 4114, Intel Xeon 6130 and Intel Xeon 6230
4110	12/20/2021	ProtectServer PCIe HSM 3	Thales	Hardware Version: 808-000048-002, 808-000073-001; Firmware Version: 7.00.01 with bootloader version 1.2.0
4111	12/20/2021	Motorola Solutions Cryptographic Software Module	Motorola Solutions, Inc.	Software Version: R01.11.00
4112	12/20/2021	Gallagher OpenSSL Cryptographic Module	Gallagher Group	Software Version: 1.1
4113	12/20/2021	FortiSandbox-1000F/2000E/3000E	Fortinet, Inc.	Hardware Version: FortiSandbox-2000E (C1AG28), FortiSandbox-1000F (C1AH16) and FortiSandbox-3000E (C1AF74) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiSandbox 3.1, build 5166
4114	12/22/2021	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
4115	12/27/2021	R650-US Access Point, R650-WW Access Point, R750 Access Point, R850 Access Point, T750SE Access Point, T750 Access Point, and T750-WW Access Point	CommScope Technologies LLC	Hardware Version: [(9F1-R650-US00, revA), (9F1-R650-WW00, revA), (9F1-R750-US00, revA), (9F1-R850-US00, revA), (9F1-T750-US51, revA), (9F1-T750-US01, revA), and (9F1-T750-WW01, revA)] with Tamper Evident Label Kit (902-FTEL-0040); Firmware Version: 5.2.1.3
4116	12/27/2021	Silver Peak Unity EdgeConnect EC-XS-FIPS, EC-M-P-FIPS, EC-XL-P-FIPS and EC-XL-P-NM-FIPS	Silver Peak Systems, Inc.	Hardware Version: EC-XS-FIPS[1], EC-M-P-FIPS[2], EC-XL-P-FIPS[3] and EC-XL-P-NM-FIPS[3] with FIPS Kit 500329-001[1], 500330-001[2] or 500331-001[3]; Firmware Version: 8.1.9.7
4117	12/28/2021	Radio Internet-Protocol Communications Module Z (RIC-Mz)	Christine Wireless, Inc.	Hardware Version: RIC-Mz Spin 4; Firmware Version: DTLS_FIPS_Final_10_31_20
4118	12/28/2021	Nutanix Cryptographic Module for BoringSSL	Nutanix, Inc.	Software Version: ae223d6138807a13006342edfeef32e813246b39