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 2020

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: Jan 14, 2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: Jan 05 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
3751	12/01/2020	WatchGuard Firebox T15[1], T15-W[2], T35[3], T35-W[4], T55[5], T55-W[6], T70[7]	WatchGuard Technologies, Inc.	Hardware Version: MS1AE3 [1]; MS1AE3W [2]; MS3AE5 [3]; MS3AE5W [4]; MS5AE5 [5]; MS5AE5W [6]; WS7AE8 [7]; FIPS Kit P/N: WG8566; Firmware Version: Fireware OS v12.3.1
3752	12/01/2020	WatchGuard Firebox M270[1], M370[2], M470[3], M570[4], M670[5]	WatchGuard Technologies, Inc.	Hardware Version: TL2AE8 [1]; WL6AE8 [2]; WL6AE8 [3-5] with WG8592, WG8593 and WG8594; FIPS Kit P/N: WG8566; Firmware Version: Fireware OS v12.3.1
3753	12/02/2020	BoringCrypto Android	Google, LLC.	Software Version: 7f02881e96e51f1873afcf384d02f782b48967ca
3754	12/02/2020	Quantum Xchange FIPS Module	Quantum Xchange	Software Version: 1.0
3755	12/03/2020	Samsung NVMe TCG Opal SSC SEDs PM1733 Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLJ1T9HBJR-000C9 [1], MZWLJ3T8HBLS-000C9 [1], MZWLJ7T6HALA-000C9 [1], MZWLJ15THALA-000C9 [1] and MZWLJ3T8HBLS-00AG6 [2]; Firmware Version: EPK90E5Q [1] and ZG5Q [2]
3756	12/03/2020	Key Variable Loader (KVL) 5000 PIKE2	Motorola Solutions, Inc.	Hardware Version: P/N 51009397004; Firmware Version: Base FW R50.05.01 or R50.07.01 with or without AES128 R01.00.01, AES256 R01.00.01, and/or ADP/DES/DES-OFB/DES-XL/DVI-XL/DVP-XL R01.00.00
3757	12/07/2020	Oracle Linux 7 GnuTLS Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
3758	12/07/2020	Phison TCG OPAL SSC SSD Series	Phison Electronics Corporation	Hardware Version: PSS12F-2.5-128G-V01 [A], PSS12F-2.5-256G-V01 [A], PSS12F-2.5-512G-V01 [A], PSS12F-2.5-1024G-V01 [A], PSS12F-2.5-2048G-V01 [A], PSS12F-M.2280D3-128G-V01 [A], PSS12F-M.2280D3-256G-V01 [A], PSS12F-M.2280D3-512G-V01 [A], PSS12F-M.2280D3-1024G-V01 [A], PSS12F-M.2280D3-2048G-V01 [A], PSS12F-M.2280S3-128G-V01 [A], PSS12F-M.2280S3-256G-V01 [A], PSS12F-M.2280S3-512G-V01 [A], PSS12F-M.2242-128G-V01 [B], PSS12F-M.2242-256G-V01 [B], PSE12F-M2280-256G-V01 [C], PSE12F-M2280-512G-V01 [C], PSE12F-M2280-1024G-V01 [C] and PSE12F-M2280-2048G-V01 [C]; Firmware Version: SCPM13.0 [A], SCQM12.0 [B] and ECPM13.0 [C]
3759	12/07/2020	Qualcomm(R) Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.5.0
3760	12/09/2020	nShield Solo XC F3 and nShield Solo XC F3 for nShield Connect XC and for nShield Issuance HSM	nCipher Security Limited	Hardware Version: NC4035E-000 and NC4335N-000, Build Standard A; Firmware Version: 12.50.11
3761	12/09/2020	SOLSDR NETNode Security Module	Domo Tactical Communications (DTC) Limited	Firmware Version: 1.0
3762	12/09/2020	Samsung Flash Memory Protector V2.0	Samsung Electronics Co., Ltd.	Software Version: 2.0; Hardware Version: FX6_V4.0 and FX6_V4.1
3763	12/10/2020	TrustedKeep Encryption Module	Trusted Concepts, Inc.	Software Version: v2.0.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3764	12/10/2020	Aruba 2930F, 2930M, 3810M and 5400R zl2 Switch Series	Hewlett Packard Enterprise	Hardware Version: Aruba 2930F Switches (JL258A, JL259A, JL260A, JL261A, JL262A, JL263A, JL264A, JL557A, JL559A and JL692A) [1], Aruba 2930M Switches (JL319A, JL320A, JL321A, JL322A, JL323A, JL324A, R0M67A and R0M68A) [1] with Expansion Cards listed in Table 3 of the Security Policy, Aruba 3810M Switches (JL071A, JL072A, JL073A, JL074A, JL075A and JL076A) [2] with Expansion Cards listed in Table 4 of the Security Policy, Aruba 5400R zl2 Switches (5406R zl2 J9821A and 5412R zl2 J9822A) [2] with Management card and Interface Cards listed in Table 5 of the Security Policy; Firmware Version: WC.16.08 [1] or KB.16.08 [2]
3765	12/10/2020	nShield Solo XC F2	nCipher Security Limited	Hardware Version: NC3025E-000, Build Standard A; Firmware Version: 12.50.11
3766	12/10/2020	nShield Solo XC F3 and nShield Solo XC F3 for nShield Connect XC and for nShield Issuance HSM	nCipher Security Limited	Hardware Version: NC4035E-000 and NC4335N-000, Build Standard A; Firmware Version: 12.50.11
3767	12/11/2020	Standalone IMB	GDC Technology (USA) LLC	Hardware Version: GDC-IMB-v6; Firmware Version: 5.0, Security Manager Firmware Version 1.8.5 and 5.1, Security Manager Firmware Version 1.8.6
3768	12/14/2020	REDCOM OpenSSL Cryptographic Module	REDCOM Laboratories, Inc.	Software Version: 1.0
3769	12/14/2020	PTP 820C, PTP 820C-HP, PTP 820C 2E2SX, PTP 820S, PTP 820N, PTP 820A, PTP 820G, and PTP 820GX	Cambium Networks	Hardware Version: [PTP 820N, PTP 820A, with components PTP820 TCC-B-MC: N000082H001, PTP820 TCC-B2: N000082H002, PTP820 TCC-B2-XG-MC: N000082H003, PTP820 RMC-B: N000082H004], [PTP 820GX with components PTP820 RMC-B: N000082H004], [PTP 820C], [PTP 820C-HP], [PTP 820C 2E2SX], [PTP 820S], [PTP 820G]; Firmware Version: PTP820 Release 10.9.6b74
3770	12/14/2020	Qualcomm(R) Trusted Execution Environment Software Cryptographic Library	Qualcomm Technologies, Inc.	Software Version: 5.8-00049; Hardware Version: Snapdragon 865 Mobile Platform
3771	12/15/2020	LifeCare PCA™ Infusion Pump	ICU Medical, Inc.	Hardware Version: P/Ns 20837-04-03 and 20837-04-04 with components 810-04505-039 and 810-11438-018; Firmware Version: CE v1.90.0.8 and MCU v7.4.0.5
3772	12/16/2020	Virtual SmartZone (vSZ) WLAN Controller	Ruckus Wireless, Inc.	Software Version: 5.1.1.3
3773	12/16/2020	Acronis SCS Cryptographic Module	Acronis SCS	Software Version: 1.0
3774	12/18/2020	SUSE Linux Enterprise Server Kernel Crypto API Cryptographic Module	SUSE, LLC	Software Version: 3.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3775	12/18/2020	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 16.9
3776	12/18/2020	IMS3-SM	Dolby Laboratories, Inc.	Hardware Version: IMS3-41 [A], IMS3-42 [A], IMS3-43 [A], IMS3C-11 [B], IMS3C-12 [B] and IMS3C-13 [B]; Firmware Version: (1.2.9-0, 1.2.9-3 and 1.2.4-0) [A], (3.3.43-0, 3.3.43-3, 3.3.43-0) [B]
3777	12/18/2020	DRAEGER WCM9113 802.11ABGN VG2	Draeger Medical Systems, Inc.	Hardware Version: MS32018 Rev. 03; Firmware Version: 1.8.2 with Bootloader versions 1.7 and 1.8
3778	12/18/2020	Postal NRevenector GB 2019	FP InovoLabs GmbH	Hardware Version: 58.0036.0301.00 and 58.0036.0302.00; Firmware Version: Bootloader 90.0036.0401.00/2019141001 and GB Application: 90.0036.0415.00/2019366001
3779	12/21/2020	Junos Space Network Management Platform, with or without Network Director and with or without Security Director in Virtual Appliance	Juniper Networks, Inc.	Software Version: Junos Space 19.1R1_FIPS, Network-Director.3.6R3.15 and Security-Director-19.1R1.23
3780	12/21/2020	RS9113	Redpine Signals, Inc.	Hardware Version: 6.0; Firmware Version: RS9113.N00.WC.FIPS.OSI.1.8.2 Bootloader version 1.8 and Bootloader Version 1.7
3781	12/21/2020	Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20200305
3782	12/21/2020	Samsung BoringSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 1.4
3783	12/21/2020	1FINITY(TM) T600 Transport Blade	Fujitsu Network Communications, Inc.	Hardware Version: T600 with Tamper Evident Seals: 246700000108A and 246700000115A; Firmware Version: t600-19.1_cd42 and t600-19.1_cd188
3784	12/21/2020	Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20190624
3785	12/30/2020	NS361/NS371/NS561 (2.5" & M.2) SSD	Novachips Co., Ltd.	Hardware Version: NS361F500GCC1-1F [04MB3], NS371F04T0CC1-1F [16MN3], NS371F08T0CC0-1F [16MN3], NS361F500GCE7-1F [04MB3] and NS561F500GCE7-1F [02MB3]; Firmware Version: NV.R1800_1200
3786	12/30/2020	Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a/PM1645a Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILT960HBHQ-00AC9 [1, 3, 5], MZILT1T9HBJR-00AC9 [1, 3, 5], MZILT3T8HBLS-00AC9 [1, 3, 5], MZILT7T6HALA-00AC9 [1, 3, 5], MZILT15THALA-00AC9 [1, 3, 5], MZILT30THALA-00AC9 [1, 3, 5], MZILT800HBHQ-00AC9 [2, 4, 6], MZILT1T6HBJR-00AC9 [2, 4, 6] and MZILT3T2HBLS-00AC9 [2, 4, 6]; Firmware Version: EXA0 [1], EZA0 [2], EXA1 [3], EZA1 [4], EXA2 [5] and EZA2 [6]

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3787	12/31/2020	Qualcomm(R) Secure Processing Unit (SPU)	Qualcomm Technologies, Inc.	Hardware Version: 4.0; Firmware Version: spss.a1.1.3_00077