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

September 2019

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: Michael Cooper

Dated: 10/3/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: October 3, 2019

Manager, Product Assurance and Standards
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
3517	09/03/2019	YubiKey 4 Cryptographic Module	Yubico, Inc.	Hardware Version: SLE78CLUFX3000PH; Firmware Version: 4.4.5
3518	09/05/2019	DocuSign Signature Appliance	DocuSign, Inc.	Hardware Version: 8.0; Firmware Version: 9.0.9.10
3519	09/05/2019	SafeNet Cryptovisor K7 Cryptographic Module	Gemalto	Hardware Version: 808-000048-002 and 808-000073-001; Firmware Version: 1.1
3520	09/05/2019	SafeNet Cryptovisor K7+ Cryptographic Module	Gemalto	Hardware Version: 808-000069-001 and 808-000070-001; Firmware Version: 1.1
3521	09/08/2019	NITROXIII CNN35XX-NFBE HSM Family	Marvell Semiconductor, Inc.	Hardware Version: CNL3560P-NFBE-G, CNL3560P-NFBE-2.0-G, CNL3560M-NFBE-2.0G, CNL3560-NFBE-G, CNL3560-NFBE-2.0-G, CNL3530-NFBE-G, CNL3530-NFBE-2.0-G, CNL3510-NFBE-G, CNL3510-NFBE-2.0-G, CNL3510P-NFBE-G, CNL3510P-NFBE-2.0-G, CNN3560P-NFBE-G, CNN3560P-NFBE-2.0-G, CNN3560-NFBE-G, CNN3560-NFBE-2.0-G, CNN3530-NFBE-G, CNN3530-NFBE-2.0-G, CNN3510-NFBE-G and CNN3510-NFBE-2.0-G; Firmware Version: CNN35XX-NFBE-FW-3.3 build 11
3522	09/09/2019	SecureUSB KP	SECUREDATA, Inc.	Hardware Version: SU-KP-BL-4, SU-KP-BL-8, SU-KP-BL-16, SU-KP-BL-32, SU-KP-BL-64; Firmware Version: V1.01.10 and (V1.11.1 or V1.12)
3523	09/10/2019	Apple Secure Key Store Cryptographic Module, v9.0	Apple Inc.	Hardware Version: 1.2[1], 2.0[2]; Firmware Version: SEPOS
3524	09/10/2019	Poly Voice Common Cryptographic Module	Poly Inc.	Software Version: 2.0.16
3525	09/12/2019	Samsung NVMe TCG Opal SSC SEDs PM1723b Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLL1T9HAJQ-000C9, MZWLL3T8HAJQ-000C9, MZWLL7T6HMLA-000C9, MZWLL15THMLA-000C9; Firmware Version: GPJ95E5Q
3526	09/16/2019	Ciena Waveserver Ai WCS-2 Module	Ciena® Corporation	Hardware Version: 186-1034-411-EB, Revision 002 with PCB P/N: 186-1034-210 Revision 001; Firmware Version: 1.3.5
3527	09/16/2019	Kernel Mode Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.15063.728
3528	09/18/2019	SecureUSB BT	SECUREDATA, Inc.	Hardware Version: SU-BT-BU-4, SU-BT-BU-8, SU-BT-BU-16, SU-BT-BU-32, SU-BT-BU-64; Firmware Version: V1.01.10 and (V2.0.8 or V2.4)
3529	09/18/2019	PL-2000M, PL-2000AD and PL-2000ADS	PacketLight Networks Ltd.	Hardware Version: PL-2000M, PL-2000AD, PL-2000ADS; Firmware Version: 1.3.12
3530	09/19/2019	Panorama 8.1 M-100, M-200, M-500 and M-600	Palo Alto Networks	Hardware Version: P/Ns 910-000030 Version 00D [1], 910-000092 Version 00D [1], 910-000176 Version 00A [2], 910-000073 Version 00D [3], and 910-000175 Version 00A [4]; FIPS Kit P/Ns 920-000140 Version 00A [1], 920-000208 Version 00A [2], 920-000145 Version 00A [3], and 920-000209 Version 00A [4]; Firmware Version: 8.1.6
3531	09/19/2019	Panorama Virtual Appliance 8.1	Palo Alto Networks	Software Version: 8.1.6

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3532	09/20/2019	FortiGate-VM Virtual Appliances	Fortinet, Inc.	Software Version: FortiGate-VM 5.4, b3276, 171006
3533	09/24/2019	VAULTIC 420 [1], 460 [2]	WISeKey Semiconductors	Hardware Version: Hardware Platform: AT90SO128 - Silicon Rev H; [1] P/N #ATVaultIC420, [2] P/N #ATVaultIC460; Firmware Version: 1.2.14
3536	09/25/2019	PA-200, PA-220, PA-220R, PA-500, PA-800 Series, PA-3000 Series, PA-3200 Ser es, PA-5000 Series, PA-5200 Ser es and PA-7000 Series Firewalls	Palo Alto Networks	Hardware Version: PA-200 P/N 910-000015 Rev. E with [1], PA-220 P/N 910-000128 Rev. A with [1], PA-220R P/N 910-000147 Rev. B with [10], PA-500 P/N 910-000006 Rev. O with [2], PA-500-2GB P/N 910-000094 Rev. O with [2], PA-820 P/N 910-000120 Rev. A with [3], PA-850 P/N 910-000119 Rev. A with [3], PA-3020 P/N 910-000017 Rev. J with [4], PA-3050 P/N 910-000016 Rev. J with [4], PA-3060 P/N 910-000104 Rev. C with [5], PA-3220 P/N 910-000162 Rev. A with [11], PA-3250 P/N 910-000163 Rev. A with [11], PA-3260 P/N 910-000164 Rev. A with [11], PA-5020 P/N 910-000010 Rev. F with [6], PA-5050 P/N 910-000009 Rev. F with [6], PA-5060 P/N 910-000008 Rev. F with [6], PA-5220 P/N 910-000132 Rev. A with [7], PA-5250 P/N 910-000131 Rev. A with [7], PA-5260 P/N 910-000125 Rev. A with [7], PA-5280 P/N 910-000157 Rev. A with [7], PA-7050 P/N 910-000102 Rev. B with [8] and at least one from [12] and PA-7080 P/N 910-000122 Rev. A with [9] and at least one from [12]; FIPS Kit: P/Ns 920-000084 Rev. A [1], 920-000005 Rev. A [2], 920-000185 Rev. A [3], 920-000081 Rev. A [4], 920-000138 Rev. A [5], 920-000037 Rev. A [6], 920-000186 Rev. A [7], 920-000112 Rev. A [8], and 920-000119 Rev. A [9], 920-000226 Rev. A [10] and 920-000212 Rev. A [11]; Network Processing Cards [12]: P/Ns 910-000028-00B, 910-000117-00A, 910-000137-00A and 910-000136-00A; Firmware Version: 8.1.3 or 8.1.6
3537	09/26/2019	Chunghwa Mobile ID Applet on TAISYS Technologies JUISE-S2	Chunghwa Telecom Co., Ltd. and Taisys Technologies Co., Ltd.	Hardware Version: 46 43; Firmware Version: 32 53; Applet: Chunghwa Mobile ID Applet v1.0
3538	09/26/2019	Red Hat Enterprise Linux OpenSSL Cryptographic Module	Red Hat(R), Inc.	Software Version: 7.0
3539	09/30/2019	Juniper Networks SRX320 Services Gateway with JUNOS 17.4R1-S1	Juniper Networks, Inc.	Hardware Version: SRX320; Firmware Version: JUNOS 17.4R1-S1
3540	09/30/2019	Juniper Networks SRX300, SRX340, SRX345, SRX550-M, SRX5400, SRX5600 and SRX5800 Services Gateways with Junos 17.4R1-S1	Juniper Networks, Inc.	Hardware Version: SRX300, SRX340, SRX345, SRX550-M, SRX5400, SRX5600 and SRX5800 with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS 17.4R1-S1