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

April 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: 05/04/2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 2021-05-03

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
3879	04/01/2021	IBM(R) NVMe FlashCore(TM) Module 2	IBM(R) Corporation	Hardware Version: 02CL181, 02CL183, 02CL185, 02CL187; Firmware Version: 2.0.9.67
3880	04/03/2021	Cisco FTD FX-OS on 4K/9K Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR4110[1], FPR4115[1], FPR4120[1], FPR4125[1], FPR4140[1], FPR4145[1], FPR4150[1], FPR9K-SM-24[2], FPR9K-SM-36[2], FPR9K-SM-40[2], FPR9K-SM-44[2], FPR9K-SM-48[2] and FPR9K-SM-56[2] with FIPS Kit (Cisco_TEL.FIPS_Kit), and opacity shield 69-100250-01[1] or 800-102843-01[2]; Firmware Version: 2.6
3881	04/03/2021	BeyondTrust Cryptographic Module	BeyondTrust Corporation	Software Version: 2.2
3882	04/05/2021	HID Global Applets v3.0 on NXP JCOP 3 SecID P60 CS (OSB)	HID Global	Hardware Version: P6022y VB with product identifier J3H145C; Firmware Version: 19790400 and HID Global ActivID Applet Suite v3.0 with factory configuration FIPS 140-2-L3
3883	04/06/2021	Cisco Catalyst 9800 (40/80/L) Wireless Controllers running IOS-XE 16.12	Cisco Systems, Inc.	Hardware Version: 9800-40, 9800-80 and 9800-L; Firmware Version: IOS-XE 16.12

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3884	04/06/2021	PAN-OS 9.0 Firewalls PA-220, PA-220R, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series	Palo Alto Networks, Inc.	Hardware Version: PA-220 P/N 910-000128 Rev. A with [1], PA-220R P/N 910-000147 Rev. B 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 [6], PA-3250 P/N 910-000163 Rev. A with [6], PA-3260 P/N 910-000164 Rev. A 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-5280-K2-EXP: P/N: 910-000257 Rev. A with [7], PA-5280-K2-SEC: P/N: 910-000357 Rev. B with [7], PA-7050 P/N 910-000102 Rev. B with [8], [12], [14] and at least one from [10]; PA-7080 P/N 910-000122 Rev. A with [9], [12], [15] and at least one from [10]; PA-7050 P/N 910-000102 Rev. B with [8], [13], one from [11] and one from [17]; PA-7080 P/N 910-000122 Rev. A with [9], [13], one from [11] and one from [16]; FIPS Kit: P/Ns 920-000084 Rev. A [1], 920-000226 Rev. A [2], 920-000185 Rev. A [3], 920-000081 Rev. A [4], 920-000138 Rev. A [5], 920-000212 Rev. A [6], 920-000186 Rev. A [7], 920-000112 Rev. A [8] and 920-000119 Rev. A [9]; Network Processing Cards [10]: P/Ns 910-000028-00B, 910-000117-00A, 910-000137-00A, 910-000136-00A, 910-000156-00A, 910-000256-00A and 910-000356-00B; Network Processing Cards [11]: P/Ns 910-000156-00A, 910-000256-00A, and 910-000356-00B; Log Processing Card [12]: P/N 910-0000014-00A; Log Forwarding Card [13]: P/N 910-000183-00A; Switch Management Card [14]: P/N 910-000013-00P; Switch Management Card [15]: P/N 910-000012-00L; Switch Management Cards [16]: P/Ns 910-000186-00A, 910-000286-00D, 910-000386-00D; Switch Management Cards [17]: P/Ns 910-000185-00A, 910-000285-00C, 910-000385-00C; Firmware Version: 9.0.9-h1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3885	04/06/2021	AT-SBx908 Gen2, AT-x950, AT-x550, AT-x530 Secure Management Module	Allied Telesis	Hardware Version: AT-SBx908 Gen2, 990-007222-F00 with [1], [2], [3], [4] [Tamper Label Kit: 066-000080 x 10, 056-000658 x 1] [A], AT-x950-28XTQm, 990-007221-F00 with [2], [5], [Tamper Label Kit: 066-000080 x 4, 056-000658 x 1] [B], AT-x950-28XSQ, 990-007712-F00 with [3], [5], [Tamper Label Kit: 066-000080 x 4, 056-000658 x 1] [B], AT-x550-18XTQ, 990-007217-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x550-18XSQ, 990-007218-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x550-18XSQ, 990-007724-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x550-18XSPQm, 990-007219-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x530-52GTXm, 990-007725-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530-52GPXm, 990-007726-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530-28GTXm, 990-007220-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530-28GPXm, 990-007727-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530L-52GTX, 990-007728-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530L-52GPX, 990-007729-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530L-28GTX, 990-007730-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D] and AT-x530L-28GPX, 990-007731-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D]; XEM2 Modules [1] 990-005492-00, 990-005490-00, 990-005493-00, 990-006024-00, 990-005491-00, XEM2 Module [2] 990-006242-00 and XEM2 Module [3] 990-006018-00; Power Supply Unit [4] 990-004783-10 and Power Supply Unit [5] 990-006195-10; Firmware Version: 5.4.9.APCERT-2.3; Bootloader Versions bl-6.2.7-SBx908NG-39A8-D2D8.bin [A], bl-6.2.20-x950-1D0D-2BC3.bin [B], bl-6.2.21-x550-2FC1-A0F1.bin [C], bl-7.0.3-x530-noecc-B495-8AEE.kwb [D]
3886	04/07/2021	CryptoServer CSe-Series	Utimaco IS GmbH	Hardware Version: CryptoServer CSe-Series 4.00.5.0 and CryptoServer CSe-Series 4.00.5.1; Firmware Version: SecurityServer-CSe-Series-4.32.0.3-FIPS
3887	04/07/2021	Integral Crypto AES 256 Bit USB 3.0	Integral Memory Plc	Hardware Version: INFD4GCRY3.0140-2, INFD8GCRY3.0140-2, INFD16GCRY3.0140-2, INFD32GCRY3.0140-2, INFD64GCRY3.0140-2, INFD128GCRY3.0140-2, INFD256GCRY3.0140-2, INFD512GCRY3.0140-2, INFD1TCRY3.0140-2, INFD2TCRY3.0140-2, INFD4GCRYDL3.0140-2, INFD8GCRYDL3.0140-2, INFD16GCRYDL3.0140-2, INFD32GCRYDL3.0140-2, INFD64GCRYDL3.0140-2, INFD128GCRYDL3.0140-2, INFD256GCRYDL3.0140-2, INFD512GCRYDL3.0140-2, INFD1TCRYDL3.0140-2, INFD2TCRYDL3.0140-2, INFD4GENVDL3.0-140, INFD8GENVDL3.0-140, INFD16GENVDL3.0-140, INFD32GENVDL3.0-140, INFD64GENVDL3.0-140, INFD128GENVDL3.0-140, INFD256GENVDL3.0-140, INFD512GENVDL3.0-140, INFD1TENVDL3.0-140, INFD2TENVDL3.0-140; Firmware Version: 4.06.10

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3888	04/09/2021	PAN-OS 9.0 VM-Series	Palo Alto Networks, Inc.	Software Version: 9.0.9-h1
3889	04/12/2021	Fortress Mesh Points	General Dynamics Mission Systems	Hardware Version: ES2440, ES520v1, ES520v2 and ES820; Firmware Version: 5.4.6
3890	04/12/2021	TippingPoint Crypto Core OpenSSL	Trend Micro Inc.	Software Version: 1.0.2l-fips
3891	04/12/2021	Red Hat Enterprise Linux 7 OpenSSH Server Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190626
3892	04/12/2021	Red Hat Enterprise Linux 7 OpenSSH Client Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190626
3893	04/15/2021	Oracle Linux Unbreakable Enterprise Kernel (UEK 5) Cryptographic Module	Oracle Corporation	Software Version: R7-5.0.0
3894	04/15/2021	Panorama Virtual Appliance 9.0	Palo Alto Networks, Inc.	Software Version: 9.0.9
3895	04/15/2021	WildFire 9.0 WF-500	Palo Alto Networks, Inc.	Hardware Version: 910-000097-00G; FIPS Kit P/N: 920-000145-00A; Firmware Version: 9.0.9-h1
3896	04/15/2021	Panorama 9.0 M-100, M-200, M-500 and M-600	Palo Alto Networks, Inc.	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: 9.0.9
3897	04/16/2021	FortiWLM-100D and FortiWLM-1000D	Fortinet, Inc.	Hardware Version: FWM-100D (C1AE82) and FWM-1000D (C1AE83) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiWLM 8.5-2fips-1
3898	04/17/2021	Luna T7 Cryptographic Module	Thales Trusted Cyber Technologies	Hardware Version: 872-500024-001 and 872-500025-001; Firmware Version: 7.11.1 with Boot Loader version 2.0.1
3899	04/19/2021	Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points with Aruba Instant Firmware	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [IAP-303H-US TAA (HPE SKU JY681A), IAP-304-US TAA (HPE SKU JX944A), IAP-305-US TAA (HPE SKU JX950A), IAP-314-US TAA (HPE SKU JW808A), IAP-315-US TAA (HPE SKU JW814A), IAP-324-US TAA (HPE SKU JW322A), IAP-325-US TAA (HPE SKU JW328A), IAP-334-US TAA (HPE SKU JW820A), IAP-335-US TAA (HPE SKU JW826A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaInstant 8.5.0.12
3900	04/19/2021	Samsung BoringSSL Android	Samsung Electronic Co. Ltd.	Software Version: 1.5
3901	04/19/2021	FIPS AP43	Mist Systems	Hardware Version: AP43-FIPS-US [REV. AA] and AP43E-FIPS-US [REV. AA]; Firmware Version: fips_apfw-0.8.20681-master-5ce6

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3902	04/20/2021	Ubuntu 20.04 Libgcrypt Cryptographic Module	Canonical Ltd.	Software Version: 3.0
3903	04/22/2021	MonoCrypt AES Enhanced Crypto Library	Focus Systems Corporation	Software Version: 2.0.0
3904	04/22/2021	TASS Crypto Engine	Beijing JN TASS Technology Co., Ltd.	Hardware Version: CE2-A2H0O4; Firmware Version: H1.00.00
3905	04/22/2021	CN Series Encryptors	Senetas Corporation Ltd., distributed by Thales SA (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. & SafeNet Inc. CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Senetas Corp. Ltd. & Thales CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. & Thales CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. & Thales CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Firmware Version: 5.1.1
3906	04/22/2021	CN6000 Series Encryptors	Senetas Corporation Ltd., distributed by Thales SA (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & Thales CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Firmware Version: 5.1.1
3907	04/22/2021	YubiKey 5 Cryptographic Module	Yubico, Inc.	Hardware Version: SLE78CLUFX3000PH and SLE78CLUFX5000PH; Firmware Version: 5.4.2
3908	04/23/2021	Juniper Networks NFX250 Network Services Platform	Juniper Networks, Inc.	Hardware Version: NFX250-S1, NFX250-S1E and NFX250-S2; Firmware Version: Junos OS 20.1R1
3909	04/26/2021	IBM(R) z/OS(R) Version 2 Release 4 ICSF PKCS #11 Cryptographic Module	IBM Corporation	Software Version: ICSF level HCR77D0 with APAR OA58593; Hardware Version: COP chips integrated within processor unit [1] and COP chips integrated within processor unit and P/N 01PP167 [2]; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 32L [1], and Feature 3863 (aka FC3863) with System Driver Level 32L and CCA 6.0.8z [2]

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3910	04/27/2021	FSM-2 Flash Storage Cryptographic Module	Curtiss-Wright Defense Solutions	Hardware Version: A8; Firmware Version: 4.0