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

May 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 A. Hall

Dated: 03 June 2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 2021-06-01

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
3911	05/03/2021	Qualcomm(R) Secure Processing Unit (SPU) Random Number Generator (RNG)	Qualcomm Technologies, Inc.	Hardware Version: 2.0
3912	05/03/2021	FortiGate-3401E/3601E/3960E/3980E	Fortinet, Inc.	Hardware Version: FortiGate-3401E (C1AH85), FortiGate-3960E (C1AF81), FortiGate-3601E (C1AH57) and FortiGate-3980E (C1AF63) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548
3913	05/03/2021	FortiGate-61E/61F/81E/101E/101F and FortiWiFi-61E	Fortinet, Inc.	Hardware Version: FortiGate-61E (C1AE14) [2] [4], FortiGate-61F (C1AJ23) [1] [3], FortiGate-81E (C1AE21) [2] [4], FortiGate-101E (C1AE27) [2] [4], FortiGate-101F (C1AJ44) [1] [3] and FortiWiFi-61E (C1AE18) [2] [4] with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.0 build 5439 [1], FortiOS 6.0 build 5445 [2], FortiOS 6.2 build 5526 [3], FortiOS 6.2 build 5548 [4]
3914	05/03/2021	YubiKey 5 Cryptographic Module	Yubico, Inc.	Hardware Version: SLE78CLUFX3000PH and SLE78CLUFX5000PH; Firmware Version: 5.4.2
3915	05/03/2021	ZOLL Cryptographic Module	ZOLL Medical Corporation	Software Version: 2.2
3916	05/03/2021	YubiHSM 2 Cryptographic Module	Yubico, Inc.	Hardware Version: SLE78CLUFX3000PH and SLE78CLUFX5000PH; Firmware Version: 2.2.0
3917	05/03/2021	HUAWEI OptiX OSN 1800 Series	Huawei Technologies Co., Ltd.	Hardware Version: OSN 1800 V (P/N 02300783), TNZ5UXCMS - System, Control and Communication Board (P/Ns 60:023GBW10J8004412 and 50:023GBW10H3000534), TNF1CE6 - WDM Interface Board (P/N 022PYL10HC000078), TNF1LDCA - WDM Interface Board (P/N 032VFR10JA000121), TNF6TTA - Client-side Optical Interface Board (P/N 031YNU10GC000362), TNZ5UNS4 - WDM-side Optical Interface Board (P/N 032AUB10JA000039), TNF6APIU - AC Power Supply (P/Ns 2102312ADY10J6000005 and 2102312ADY10J6000011), TNF5PIU - DC Power Supply (P/Ns 021YNWD0K1001350 and 021YNWD0J8001151), TNFK01AFB - Backplane Board (P/N 2102300783N0JB000695), TNF5FAN - Fan (P/N 2102120877N0JB000647); OSN 1800 IIE (P/N 02301163), TNZ2UXCL - System, Control and Communication Board (P/Ns 023VFQ10J8000390 and 023VFQ10J8000392), TNF1CE6 - WDM Interface Board (P/N 022PYL10HC000078), TNF1LDCA - WDM Interface Board (032VFR10JA000121), TNZ1APIU - AC Power Supply (P/N A1163190103002V0 and A1163190103010V0), ANK1PIU - DC Power Supply (P/Ns 023NKNLUJA010598 and 023NKNLUJA010621), TNZ2K01AFB - Backplane Board (P/N 2102301163N0JB000002), TNZ1FAN - Fan (P/N 032MUSN0JB000002); Tamper-Evident Seal (P/N Y4697666); Firmware Version: V100R009C00SPC300 5.67.09.16T26

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3918	05/03/2021	Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20200327
3919	05/03/2021	IBM(R) z/OS(R) Version 2 Release 4 System SSL Cryptographic Module	IBM Corporation	Software Version: HCPT440/JCPT441 with APAR OA59268; Hardware Version: COP chips integrated within processor unit; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 32L
3920	05/03/2021	BCM58200 Series: BCM58201, BCM58202	Broadcom, Inc.	Hardware Version: P/Ns BCM58201A0KFBG and BCM58202PA0KFBG; Firmware Version: 1.1.0 with hash ID e4ef4c0cd87e42d6ae0e567347c78e22efadba5c
3921	05/04/2021	Oracle Linux Unbreakable Enterprise Kernel (UEK 4) Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
3922	05/09/2021	SUSE Linux Enterprise Server NSS Cryptographic Module	SUSE, LLC	Software Version: 3.0
3923	05/10/2021	Boot Manager	Microsoft Corporation	Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3]
3924	05/10/2021	IBM(R) z/OS(R) Version 2 Release 4 ICSF PKCS #11 Cryptographic Module	IBM Corporation	Software Version: ICSF level HCR77D0 with APAR OA59040; Hardware Version: COP chips integrated within processor unit [1] and COP chips integrated within processor unit and P/N 02WN654-N37880 (Low Power) [2]; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 41C [1], and Feature 3863 (aka FC3863) with System Driver Level 41C and CCA 7.0.68z [2]
3925	05/10/2021	CryptoServer Se-Series Gen2	Utimaco IS GmbH	Hardware Version: [CryptoServer Se-Series Gen2 5.01.2.0, CryptoServer Se-Series Gen2 5.01.4.0, and CryptoServer Se-Series Gen2 5.01.4.2] and optional component: crypto accelerator Exar DX8204; Firmware Version: SecurityServer-Se2-Series-4.32.0.3-FIPS
3926	05/11/2021	DIGISTOR TCG OPAL SSC FIPS SSD Series	DIGISTOR	Hardware Version: DIG-SSD21286-SI [A], DIG-SSD22566-SI [A], DIG-SSD25126-SI [A], DIG-SSD210006-SI [A], DIG-SSD220006-SI [A], DIG-M21286-SI [A], DIG-M22566-SI [A], DIG-M25126-SI [A], DIG-M210006-SI [A], DIG-M220006-SI [A], DIG-M2N22566-UI [B], DIG-M2N25126-UI [B], DIG-M2N210006-UI [B], DIG-M2N220006-UI [B]; Firmware Version: SCPG13.0 [A] and ECPG13.0 [B]
3927	05/17/2021	FortiGate-201E/301E/401E/501E/601E	Fortinet, Inc.	Hardware Version: FortiGate-201E (C1AE64), FortiGate-301E (C1AG46), FortiGate-401E (C1AH76), FortiGate-501E (C1AG44) and FortiGate-601E (C1AH71) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548
3928	05/19/2021	Ubuntu 20.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 3.0
3929	05/21/2021	Poly Unified Communications Cryptographic Module	Plantronics, Inc.	Hardware Version: Qualcomm Snapdragon 835 and NXP i.MX 8M; Firmware Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3930	05/21/2021	NITROXIII CNN35XX-NFBE HSM Family	Marvell	Hardware Version: P/Ns CNL3560P-NFBE-G, CNL3560-NFBE-G, CNL3530-NFBE-G, CNL3510-NFBE-G, CNL3510P-NFBE-G, CNN3560P-NFBE-G, CNN3560-NFBE-G, CNN3530-NFBE-G and CNN3510-NFBE-G, Version HW-1.0; CNL3560P-NFBE-2.0-G, CNL3560-NFBE-2.0-G, CNL3530-NFBE-2.0-G, CNL3510-NFBE-2.0-G, CNL3510P-NFBE-2.0-G, CNL3560PB-NFBE-2.0-G, CNL3560B-NFBE-2.0-G, CNL3530B-NFBE-2.0-G, CNL3510B-NFBE-2.0-G, CNL3510PB-NFBE-2.0-G, CNN3510LP-NFBE-2.0-G, CNN3510LPB-NFBE-2.0-G, CNN3560P-NFBE-2.0-G, CNN3560-NFBE-2.0-G, CNN3530-NFBE-2.0-G, CNN3510-NFBE-2.0-G and CNN3505LP-NFBE-2.0-G, Version HW-2.0; CNL3560P-NFBE-3.0-G, CNL3560B-NFBE-3.0-G, CNL3560-NFBE-3.0-G, CNL3560A-NFBE-3.0-G, CNL3560C-NFBE-3.0-G, CNL3560D-NFBE-3.0-G, CNL3560E-NFBE-3.0-G, CNL3560F-NFBE-3.0-G, CNL3560I-NFBE-3.0-G , CNL3530-NFBE-3.0-G, CNL3530B-NFBE-3.0-G, CNL3530A-NFBE-3.0-G, CNL3530C-NFBE-3.0-G, CNL3530D-NFBE-3.0-G, CNL3530E-NFBE-3.0-G, CNL3530F-NFBE-3.0-G, CNL3530I-NFBE-3.0-G , CNL3510-NFBE-3.0-G, CNL3510P-NFBE-3.0-G, CNL3510A-NFBE-3.0-G, CNL3510C-NFBE-3.0-G, CNL3510D-NFBE-3.0-G, CNL3510E-NFBE-3.0-G, CNL3510F-NFBE-3.0-G, CNL3510I-NFBE-3.0-G, CNN3560P-NFBE-3.0-G, CNN3560-NFBE-3.0-G, CNN3560A-NFBE-3.0-G, CNN3560C-NFBE-3.0-G, CNN3560D-NFBE-3.0-G, CNN3560E-NFBE-3.0-G, CNN3560F-NFBE-3.0-G, CNN3530-NFBE-3.0-G, CNN3530A-NFBE-3.0-G, CNN3530C-NFBE-3.0-G, CNN3530D-NFBE-3.0-G, CNN3530E-NFBE-3.0-G, CNN3530F-NFBE-3.0-G, CNN3510-NFBE-3.0-G, CNN3510A-NFBE-3.0-G, CNN3510C-NFBE-3.0-G, CNN3510D-NFBE-3.0-G, CNN3510E-NFBE-3.0-G, CNN3510F-NFBE-3.0-G, CNN3510LP-NFBE-3.0-G, CNN3510LPB-NFBE-3.0-G, CNN3510LPA-NFBE-3.0-G, CNN3510LPC-NFBE-3.0-G, CNN3510LPD-NFBE-3.0-G, CNN3510LPE-NFBE-3.0-G, CNN3510LPF-NFBE-3.0-G, CNN3505LP-NFBE-3.0-G, CNN3505LPA-NFBE-3.0-G, CNN3505LPC-NFBE-3.0-G, CNN3505LPD-NFBE-3.0-G, CNN3505LPE-NFBE-3.0-G, and CNN3505LPF-NFBE-3.0-G, Version HW-3.0; Firmware Version: CNN35XX-NFBE-FW-2.06 build 05, CNN35XX-NFBE-FW-2.06 build 06, CNN35XX-NFBE-FW-2.06 build 07 and CNN35XX-NFBE-FW-2.07 build 08
3931	05/24/2021	Aruba 9004 Series Gateway with ArubaOS FIPS Firmware	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [Aruba 9004-USF1 (HPE SKU R1B25A) and Aruba 9004-RWF1 (HPE SKU R1B26A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaOS 8.6.0.7-FIPS

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3932	05/24/2021	ENFORCER R1	Private Machines Inc.	Hardware Version: (ENFORCER.R1.A2SDi.1.0.0, ENFORCER.R1.X10SDV.1.0.0, ENFORCER.R1.M11SDV.1.0.0 or ENFORCER.R1.X11SDV.1.0.0) and other excluded components identified in Security Policy Section 1.4; Firmware Version: Security Anchor Firmware 1.2.0, Libdrbg 1.0.2, and Libucl 2.5.13
3933	05/26/2021	NPCT7xx TPM 2.0 rev 1.38	Nuvoton Technology Corporation	Hardware Version: LAG019 in TSSOP28 Package, LAG019 in QFN32 Package, and LAG019 in UQFN16 Package; Firmware Version: 7.2.2.0
3934	05/26/2021	Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE1800 Routing Engine and Multiservices MPC	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960 with components identified in Security Policy Table 1; Firmware Version: Junos OS 19.1R2
3935	05/26/2021	Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE1800 Routing Engine and MPC7E-10G MACsec Card	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960 with components identified in Security Policy Table 1; Firmware Version: Junos OS 19.1R2
3936	05/26/2021	Juniper Networks MX104 3D Universal Edge Router with the Multiservices MIC	Juniper Networks, Inc.	Hardware Version: MX104 with RE-MX104 and MS-MIC-16G; Firmware Version: Junos OS 19.1R2
3937	05/26/2021	IBM(R) z/OS(R) Version 2 Release 4 System SSL Cryptographic Module	IBM Corporation	Software Version: HCPT440/JCPT441 with APAR OA59268; Hardware Version: COP chips integrated within processor unit; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 41C
3938	05/27/2021	Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers and EX9204, EX9208, EX9214 Ethernet Switches with RE-S-X6-64G/RE-S-X6-128G/EX9200-RE2 Routing Engine and MPC7E-10G/EX9200-40XS MACsec Card	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960, EX9204, EX9208, EX9214 with components identified in Security Policy Table 1; Firmware Version: Junos OS 19.1R2