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

January 2023

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: 2023.02.01 16:12:00 -05'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall

Digitally signed by King, Lyall
DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall"
Reason: I am approving this document
Location:
Date: 2023.02.01 15:43:28-05'00'
Foxit PDF Editor Version: 12.1.0

Dated:

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
4403	01/03/2023	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
4404	01/04/2023	IBM Cloud Object Storage System's™ FIPS Cryptographic Module	IBM Corporation	Software Version: 2.0
4405	01/04/2023	Pensando Crypto Engine	Pensando Systems, Inc	Software Version: 1.0; Hardware Version: 1.0
4406	01/04/2023	FunOS Crypto Module	Fungible, Inc.	Software Version: 1.0.0; Hardware Version: F1 rev A0 and S1 rev A0
4407	01/04/2023	BoringCrypto	Google, LLC.	Software Version: 853ca1ea1168dff08011e5d42d94609cc0ca2e27
4408	01/08/2023	Cryptographic Module for BIG-IP (R)	F5, Inc.	Software Version: 14.1.4.2
4409	01/09/2023	KeyVault Hardware Security Module (kvHSM)	WiSECURE Technologies	Hardware Version: KV-HSM_V02; Firmware Version: v1.00.0000
4410	01/09/2023	SK hynix PE8111 E1.L NVMe TCG Opal SSC SED	SK hynix Inc.	Hardware Version: P/Ns HFS15T3DFMX098N [1], HFS15T3DFLX098N [1] and HFS15T3DFMX130N [2]; Firmware Version: 31180A10 [1] and 31280A10 [2]
4411	01/12/2023	NPCT7xx TPM 2.0 rev 1.59	Nuvoton Technology Corporation	Hardware Version: LAG019 in TSSOP28 Package, LAG019 in QFN32 Package, and LAG019 in UQFN16 Package; Firmware Version: 7.2.3.0, 7.2.3.1
4412	01/14/2023	STAR-2000-3	JoveAI Innovation, Inc.	Hardware Version: JV00002-03-1B-2; Firmware Version: 1.0.0.1
4413	01/16/2023	Red Hat Enterprise Linux 8 NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20201215
4414	01/16/2023	F5(R) vCMP Cryptographic Module	F5, Inc.	Firmware Version: 15.1.2.1 EHF
4415	01/16/2023	FortiGate-VM 6.4 and 7.0	Fortinet, Inc.	Software Version: FortiOS 6.4 (FIPS-CC-64-5) and FortiOS 7.0 (FIPS-CC-70-6); Hardware Version: Intel® Xeon® D-1559, Intel® Xeon® E3-1515M and Intel® Xeon® E-2276ME
4416	01/18/2023	BC-FNA (Bouncy Castle FIPS .NET API)	Legion of the Bouncy Castle Inc.	Software Version: 1.0.2
4417	01/18/2023	F5(R) Device Cryptographic Module	F5, Inc.	Hardware Version: BIG-IP i4600, BIG-IP i4800, BIG-IP i5600, BIG-IP i5800, BIG-IP i5820-DF, BIG-IP i7600, BIG-IP i7800, BIG-IP i7820-DF, BIG-IP i10600, BIG-IP i10800, BIG-IP i11600-DS, BIG-IP i11800-DS, BIG-IP i15600, BIG-IP i15800, BIG-IP 10350v-F, VIPRION B2250, VIPRION B4450 with FIPS Kit P/N: F5-ADD-BIG-FIPS140; Firmware Version: 15.1.2.1 EHF
4418	01/20/2023	Cryptographic Module for BIG-IP (R)	F5, Inc.	Software Version: 15.1.2.1 EHF
4419	01/20/2023	MagicCryptoMVP	Dream Security Co., Ltd.	Software Version: 1.0.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4420	01/20/2023	Aegis Secure Key 3Z and Aegis Secure Key 3NX Cryptographic Module	Apricorn	Hardware Version: P/Ns ASK3Z-16GB, ASK3Z-32GB, ASK3Z-64GB, ASK3Z-128GB, ASK3Z-256GB, ASK3-NX-2GB, ASK3-NX-4GB, ASK3-NX-8GB, ASK3-NX-16GB , ASK3-NX-32GB, ASK3-NX-64GB, ASK3-NX-128GB, ASK3-NX-256GB, ASK3-NXC-4GB, ASK3-NXC-8GB, ASK3-NXC-16GB, ASK3-NXC-32GB, ASK3-NXC-64GB, ASK3-NXC-128GB and ASK3-NXC-256GB; Hardware Version: Rev 1.0; Firmware Version: 1.9
4421	01/20/2023	Microchip Trust Anchor TA100	Microchip Technology Inc	Hardware Version: [TA100-Y230C2X01 and TA100T-Y230C2X01, Revision 59V01B5] [1] and [TA100-Y240C2X01, TA100T-Y240C2X01, TA100-Y240D3X01 and TA100-Y240UFB01, Revision 59V01B6] [2]; Firmware Version: [CP ROM Version 0x0006, ACE ROM Version 0x04 and DevUpdate Version 0x00B50002] [1] and [CP ROM Version 0x0007, ACE ROM Version 0x04, DevUpdate Version 0x00B60001] [2]
4422	01/23/2023	FEITIAN MFA Cryptographic Module	FEITIAN Technologies US, Inc.	Hardware Version: SLE78CLUFX5000PH; Firmware Version: 7.04
4423	01/23/2023	Type 3 Data Encryption Device (V3K-102)	Viasat, Inc.	Hardware Version: P/Ns 1090927, Versions 002, 003, 004, 005; 1163385, Versions 001 and 002; Firmware Version: 1.5.3
4424	01/25/2023	Cisco Catalyst 9800 (40/80) Wireless Controllers	Cisco Systems, Inc.	Hardware Version: 9800-40 and 9800-80; Firmware Version: IOS-XE 17.3
4425	01/26/2023	Inline Crypto Engine (ICE)	Google, LLC	Hardware Version: 1.0
4426	01/26/2023	Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module	Google, LLC	Hardware Version: 2.3.1
4427	01/27/2023	3e-520 Secure Access Point Cryptographic Module	Ultra Intelligence & Communications	Hardware Version: 1.0; Firmware Version: 5.1
4428	01/27/2023	Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20210628
4429	01/27/2023	Thales CipherTrust Cryptographic Provider (CCP)	Thales	Software Version: 1.0; Hardware Version: Intel Xeon Gold 6134
4430	01/27/2023	Thales CipherTrust Manager Core Security Module	Thales	Software Version: 1.0.3