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

July 2024

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: 2024.08.06 10:22:28 -04'00'

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: 2024.08.05 13:01:54-04'00'
Foxit PDF Editor Version: 12.1.2

Dated: _____

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
4715	07/08/2024	Palo Alto Networks SD-WAN ION Core Crypto Module	Palo Alto Networks, Inc.	Software Version: 1.0
4716	07/09/2024	Cryptographic Module for BIG-IP (R)	F5, Inc.	Software Version: 1.0.2u-fips
4718	07/11/2024	wolfCrypt	wolfSSL Inc.	Software Version: 5.2.1
4719	07/11/2024	Palo Alto Networks SD-WAN Instant-On Network (ION) Devices ION 1200, ION 1200-S, ION 3200, ION 5200, and ION 9200	Palo Alto Networks, Inc.	Hardware Version: [ION 1200, ION 1200-C-NA, ION 1200-C-ROW, ION 1200-C-5G-WW, ION 1200-S, ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW, ION 3200] with FIPS Kit P/N 920-000363, and [ION 5200 and ION 9200] with FIPS Kit P/N 920-000333; Firmware Version: 6.1.2
4720	07/11/2024	Tensor G2 UFS Inline Storage Encryption Cryptographic Module	Google, LLC	Software Version: 1.2.0; Hardware Version: 4.1.0
4721	07/11/2024	SecureSyncGuard	Safran Trusted 4D Inc.	Software Version: 2.1.2
4722	07/11/2024	SUSE Linux Enterprise Libgcrypt Cryptographic Module	SUSE, LLC	Software Version: 3.2
4723	07/11/2024	AMD ASP Cryptographic CoProcessor ("Phoenix")	Advanced Micro Devices (AMD)	Hardware Version: bc0d0443FIPS001; Firmware Version: bc0d0443FIPS001
4724	07/11/2024	KeyPair FIPS Provider for OpenSSL 3	KeyPair Consulting Inc.	Software Version: 3.0.10 with KP_1.2
4725	07/12/2024	SUSE Linux Enterprise OpenSSL Cryptographic Module	SUSE, LLC	Software Version: 4.2
4726	07/12/2024	Android Kernel Cryptographic Module	Google, LLC.	Software Version: 5.10.66-android12-9-00072-g143ac63130f0-ab7955824
4727	07/15/2024	SUSE Linux Enterprise Kernel Crypto API Cryptographic Module	SUSE, LLC	Software Version: 3.3[1] and 3.4[2]
4728	07/17/2024	SUSE Linux Enterprise NSS Cryptographic Module	SUSE LLC	Software Version: 3.1
4729	07/18/2024	Linux OpenSSL FIPS Provider	KAYTUS SYSTEM PTE. LTD.	Software Version: 3.1
4730	07/18/2024	Motorola Solutions Cryptographic Firmware Module	Motorola Solutions, Inc.	Firmware Version: R01.13.00
4731	07/19/2024	NetApp CryptoMod	NetApp, Inc.	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
4732	07/22/2024	Qualcomm(R) Pseudo Random Number Generator	Qualcomm Technologies, Inc.	Hardware Version: 3.0.0; Firmware Version: 79f3650da911b60d69384fc282c3d366a1a31bb1d1 ad17855970b5655a491fadd258ddd44163c90afe68b 7a1766da625533f1f12e9819dade4cdf913dd7138d , 3baa04170e303e524a1d7b47675098e13bb84f3158c 559d0883ed6e8ab27fd5ddd258ddd44163c90afe68b 7a1766da625533f1f12e9819dade4cdf913dd7138d and b332427132413a158e4250ec1ad69a9ded524135369 2905b39b9a3e981e6f9a4dd258ddd44163c90afe68b7 a1766da625533f1f12e9819dade4cdf913dd7138d
4733	07/22/2024	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 i15820-DF, VIPRION B2250, VIPRION B4450; Firmware Version: 16.1.3.1
4734	07/22/2024	Firepower Next-Generation IPS Virtual VMware Cryptographic Module	Cisco Systems, Inc.	Software Version: 7.0.5
4735	07/23/2024	BoringCrypto	Google, LLC.	Software Version: 2022061300
4736	07/23/2024	cPacket Crypto Module	cPacket Networks Inc.	Software Version: 2.1.2
4737	07/25/2024	Trusted Platform Module ST33KTPM2XSPI / ST33KTPM2X / ST33KTPM2A / ST33KTPM2I	STMicroelectronics	Hardware Version: P/Ns ST33KTPM2XSPI [A, C], ST33KTPM2X [A], ST33KTPM2A [B] and ST33KTPM2I [B]; Firmware Version: 9.257 [A], 10.257 [B], 9.258 [C]
4738	07/25/2024	Qualcomm® Inline Crypto Engine (UFS)	Qualcomm Technologies, Inc.	Hardware Version: 3.2.0[1], 3.2.1[2], 4.0.1[3] and 4.0.2[4]
4739	07/25/2024	Oracle Linux 8 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module and Oracle Linux 9 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module	Oracle Corporation	Software Version: kernel 5.15.0-101.103.2.1.el8uek and 5.15.0-101.103.2.1.el9uek; libkcapi 1.2.0-2.0.1.el8 and libkcapi-1.3.1-3.0.1.el9
4740	07/26/2024	CipherTrust Transparent Encryption Cryptographic Module	Thales	
4741	07/26/2024	Palo Alto Networks Core Crypto Module	Palo Alto Networks, Inc.	Software Version: 1.0
4742	07/26/2024	SUSE Linux Enterprise GnuTLS Cryptographic Module	SUSE, LLC	Software Version: 1.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4743	07/29/2024	BC-FJA (Bouncy Castle FIPS Java API)	Legion of the Bouncy Castle Inc.	Software Version: 2.0.0
4744	07/29/2024	Linux Kernel FIPS Object Module (KFOM) Cryptographic Module	Cisco Systems, Inc.	Hardware Version: ARMv8 Cortex-A53, Intel Xeon Gold 6138; Firmware Version: 1.0
4745	07/31/2024	nShield 5s Hardware Security Module	Entrust	Hardware Version: PCA10005-01 revision 03 and 04; Firmware Version: primary-version 13.2.4; recovery-version 13.2.4; uboot-version 1.1.0
4746	07/31/2024	Red Hat Enterprise Linux 9 OpenSSL FIPS Provider	Red Hat(R), Inc.	Software Version: 3.0.1-3f45e68ee408cd9c