FIPS 140 Series Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Canadian Centre for Cyber Security

September 2024

The National Institute of Standards and Technology, as the United States FIPS 140 Series Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140 Series Cryptographic Module Validation Authority; hereby validate the FIPS 140 Series testing results of the cryptographic modules listed below. The FIPS 140 Series specify 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 the FIPS 140 Series 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.

The FIPS 140 Series 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 the areas of a cryptographic module that are related to its secure design and implementation.

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: 2024.10.12 10:56:51 -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 with my legally binding signature
Location:
Date: 2024.10.11 14:26:52-04'00'
Foxit PDF Editor Version: 13.1.3

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
4775	09/03/2024	Junos® OS Evolved OpenSSL Cryptographic Module	Juniper Networks, Inc.	Software Version: 3.0.8
4776	09/03/2024	Junos® OS Evolved Kernel Cryptographic Module	Juniper Networks, Inc.	Software Version: 2.0
4785	09/03/2024	Canon MFP Security Chip	Canon Inc.	Hardware Version: 3.0; Firmware Version: 3.00, 3.00(V05L00), 3.00(V05L01)
4786	09/03/2024	KIOXIA TCG OPAL SSC Crypto Sub-Chip TC58NC1132GTC	KIOXIA Corporation	Software Version: N/A; Hardware Version: TC58NC1132GTC CRPT module 0001; Firmware Version: SC02AN
4787	09/03/2024	Samsung CryptoCore Cryptographic Module	Samsung Electronics Co., Ltd.	
4788	09/04/2024	Masimo Cryptographic Module	Masimo Corporation	Software Version: 1.0
4789	09/06/2024	IBM DataPower FIPS Provider	IBM	Software Version: 3.0.9-B3346E1D91BA83B7BAB52F472F3E6A0D
4790	09/06/2024	Arista Crypto Module v3.0 [Software, Software IPsec]	Arista Networks, Inc.	Software Version: 3.0
4791	09/06/2024	Arista Crypto Module v3.0 [Software, Software IPsec, Web Portal]	Arista Networks, Inc.	Software Version: 3.0
4792	09/10/2024	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.7
4793	09/10/2024	Canonical Ltd. Ubuntu 22.04 Libgcrypt Cryptographic Module	Canonical Ltd.	Software Version: 1.9.4-3ubuntu3+Fips1.2
4794	09/11/2024	Canonical Ltd. Ubuntu 22.04 OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 3.0.5-0ubuntu0.1+Fips2.1
4795	09/11/2024	Port Authority Series	Communication Devices Inc.	Hardware Version: PA111-SA CDI 01-03-0912I; PA111-RM CDI 01-03-0912I; PA121-RM CDI 01-03-0912I; PA155-RM CDI 01-03-0912I; PA199-RM CDI 01-03-0912I; Firmware Version: 1.0.0
4796	09/11/2024	Red Hat Enterprise Linux 9 Kernel Cryptographic API	Red Hat(R), Inc.	Software Version: 5.14.0-70.53.1.el9_0; 1.3.1-3.el9
4797	09/13/2024	Inline Crypto Engine (ICE)	Google, LLC	Hardware Version: 1.0
4798	09/13/2024	Integrated Management Complex (IMC) and B227 True Random Number Generator (TRNG) Firmware-Hybrid Cryptographic Module	Google, LLC	Hardware Version: 3.00b; Firmware Version: 20240510
4799	09/13/2024	Look-aside Cryptography and Compression Engine (LCE)	Google, LLC	Hardware Version: 3.0; Firmware Version: FW 6172
4800	09/16/2024	PQCryptoLib	PQShield LTD	Software Version: 1.0.0; Hardware Version: N/A; Firmware Version: N/A

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4801	09/16/2024	Oracle Linux 9 NSS Cryptographic Module	Oracle Corporation	Software Version: 4.35.0-381552536e763d0c
4802	09/16/2024	Ultrastar DC HC560 TCG Enterprise HDD SED, Ultrastar DC HC570 TCG Enterprise HDD SED	Western Digital Technologies, Inc.	Hardware Version: 0F38603, 0F38653, 0F48003, 0F48053; Firmware Version: RY07, R5G4, RG01, VM18, R7J4
4803	09/18/2024	IM TCG Opal SSC SSD Series	Intelligent Memory EMEA GmbH	Hardware Version: IMS325B3M1B3A1C3B3F2000 [A], IMS325B3M1B3A1I3B3F2000 [A], IMS325B5M1B3A1C3B5F2000 [A], IMS325B5M1B3A1I3B5F2000 [A], IMS325B7M1B3A1C3B7F2000 [A], IMS325B7M1B3A1I3B7F2000 [A], IMS325B9M1B3A1C3B9F2000 [A], IMS325B9M1B3A1I3B9F2000 [A], IMS3M8B3M1B3A1C3B3F2000 [A], IMS3M8B3M1B3A1I3B3F2000 [A], IMS3M8B5M1B3A1C3B5F2000 [A], IMS3M8B5M1B3A1I3B5F2000 [A], IMS3M8B7M1B3A1C3B7F2000 [A], IMS3M8B7M1B3A1I3B7F2000 [A], IMS3M8B9M1B3A1C3B9F2000 [A], IMS3M8B9M1B3A1I3B9F2000 [A], IMP3M8B3E1B3A1C3B3F2000 [B], IMP3M8B3E1B3A1I3B3F2000 [B], IMP3M8B5E1B3A1C3B5F2000 [B], IMP3M8B5E1B3A1I3B5F2000 [B], IMP3M8B7E1B3A1C3B7F2000 [B], IMP3M8B7E1B3A1I3B7F2000 [B], IMP3M8B9E1B3A1C3B9F2000 [B], IMP3M8B9E1B3A1I3B9F2000 [B], IMS325B3M1A2A1C3B3F2000 [C], IMS325B3M1A2A1I3B3F2000 [C], IMS325B5M1A2A1C3B5F2000 [C], IMS325B5M1A2A1I3B5F2000 [C], IMS325B7M1A2A1C3B7F2000 [C], IMS325B7M1A2A1I3B7F2000 [C], IMS325B9M1A2A1C3B9F2000 [C], IMS325B9M1A2A1I3B9F2000 [C], IMS3M8B3M1A2A1C3B3F2000 [C], IMS3M8B3M1A2A1I3B3F2000 [C], IMS3M8B5M1A2A1C3B3F2000 [C], IMS3M8B5M1A2A1I3B3F2000 [C], IMS3M8B7M1A2A1C3B7F2000 [C], IMS3M8B7M1A2A1I3B7F2000 [C], IMS3M8B9M1A2A1C3B9F2000 [C], IMS3M8B9M1A2A1I3B9F2000 [C], IMP3M8B3E1A2A1C3B3F2000 [D], IMP3M8B3E1A2A1I3B3F2000 [D], IMP3M8B5E1A2A1C3B5F2000 [D], IMP3M8B5E1A2A1I3B5F2000 [D], IMP3M8B7E1A2A1C3B7F2000 [D], IMP3M8B7E1A2A1I3B7F2000 [D], IMP3M8B9E1A2A1C3B9F2000 [D] and IMP3M8B9E1A2A1I3B9F2000 [D]; Firmware Version: SCPM13.0 [A], ECPM13.0 [B], SCPM15.0 [C] and ECPM15.0 [D]
4804	09/19/2024	Red Hat Enterprise Linux 8 Kernel Cryptographic API	Red Hat(R), Inc.	Software Version: 4.18.0-372.52.1.el8_6; libkcapi 1.2.0-2.el8
4805	09/23/2024	Panorama Virtual Appliance 10.1	Palo Alto Networks, Inc.	Software Version: 10.1.5
4806	09/23/2024	Panorama 10.1 on Hardware Appliances	Palo Alto Networks, Inc.	Hardware Version: 910-000176 with FIPS Kit 920-000208, 910-000073 with FIPS Kit 920-000145, 910-000175 with FIPS Kit 920-000209; Firmware Version: 10.1.5
4807	09/23/2024	WildFire 10.1 WF-500	Palo Alto Networks, Inc.	Hardware Version: 910-000097 with Physical Kit 920-000145; Firmware Version: 10.1.5

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4808	09/23/2024	Amazon Linux 2023 Kernel Cryptographic API	Amazon Web Services, Inc.	Software Version: kernel 6.1.41-64.118.amzn2023, 6.1.41-64.118.fips.amzn2023; libkcapi 1.4.0-105.amzn2023
4809	09/23/2024	Qualcomm® Trusted Execution Environment (TEE) Software Cryptographic Library	Qualcomm Technologies, Inc.	Software Version: 513b121d8d789b1e5a7fd22743994650a94b222d108c33b0d82c98ff282bac64; Hardware Version: 513b121d8d789b1e5a7fd22743994650a94b222d108c33b0d82c98ff282bac64
4810	09/23/2024	Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module	Google, LLC	Hardware Version: 2.3.1
4811	09/24/2024	OpenSSL FIPS Provider	The OpenSSL Project	Software Version: 3.0.8, 3.0.9
4812	09/24/2024	Tablo Medical Informatics System	Outset Medical, Inc.	Hardware Version: 1.0; Firmware Version: 4.9.12.6269
4813	09/24/2024	Toshiba Secure TCG Opal SSC Self-Encrypting Drive Series MG09SCP18TA and MG09SCP16TA	Toshiba Electronic Devices & Storage Corporation	Software Version: N/A; Hardware Version: A0 with MG09SCP18TA and A0 with MG09SCP16TA; Firmware Version: PC82
4815	09/26/2024	VMware VMkernel Cryptographic Module 2.0	VMware, Inc.	Software Version: 2.0