FIPS 140-2 Consolidated Validation Certificate



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





November 2020

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 | Signed on behalf of the Government of Canada | |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------|--|
| Signature: <u>Javin O'Brisn</u> | Signature: | |
| Dated: January 4, 2021 | Dated:December 21, 2020 | |
| Chief, Computer Security Division National Institute of Standards and Technology | 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 |
|-----------------------|------------------------------|----------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3742 | 11/13/2020 | Samsung NVMe TCG Opal SSC SEDs PM983 Series | Samsung Electronics Co., Ltd. | Hardware Version: MZ1LB960HAJQ-00AHE [1], MZ1LB1T9HALS-00AHE [1] and MZ1LB3T8HMLA-00AHE [2]; Firmware Version: EDA700AQ [1] and EDB700AQ [2] |
| 3743 | 11/16/2020 | RSA BSAFE(R) Crypto-C Micro Edition | RSA Security, LLC | Software Version: 4.1.4 |
| 3744 | 11/17/2020 | Juniper Networks EX2300, EX2300-C and EX3400 Ethernet Switches | Juniper Networks, Inc. | Hardware Version: EX2300-C-12P, EX2300-C-12T, EX2300-24P, EX2300-24T, EX2300-48P, EX2300-48T, EX3400-24P, EX3400-24T, EX3400-48P and EX3400-48T; Firmware Version: Junos OS 19.1R2 |
| 3745 | 11/23/2020 | Samsung Kernel Cryptographic Module | Samsung Electronics Co., Ltd. | Software Version: 2.1 and 2.1.1 |
| 3746 | 11/23/2020 | JCOP4 P71 | NXP Semiconductors | Hardware Version: [P71D321 (N7121 B1)]; Firmware Version: [Platform ID 4A335233353130323336333130343030DCE5C19CFE6D0DCF and ROM ID 2E5AD88409C9BADB and Patch ID 1 and FIPS Applet 1.0 (RC2)] |
| 3747 | 11/24/2020 | Trusted Platform Module 2.0 SLI / SLM 9670 | Infineon Technologies AG | Hardware Version: SLI 9670 (Package PG-VQFN-32-13) and SLM 9670 (Package PG-VQFN-32-13); Firmware Version: 13.11 |
| 3748 | 11/24/2020 | Ubuntu 18.04 Libgcrypt Cryptographic Module | Canonical Ltd. | Software Version: 1.0 |
| 3749 | 11/25/2020 | mTera Universal Transport Platform | Infinera Corporation | Hardware Version: 81.71S-MTERA-R6 with tamper-evident labels MKS-MSECTAPE-00; Firmware Version: FP5.1.2 |
| 3750 | 11/30/2020 | Memkor MKD-O2F 2.5"/M.2/U.2 SSD | Memkor, Inc. | Hardware Version: MKD25ST250IN-O2FA, MKD25ST500IN-O2FA, MKD25ST250IN-O2FB, MKD25ST1T0IN-O2FA, MKD25ST4T0IO-O2FA, MKD25P41T0IO-O2FA, MKD25P44T0IO-O2FA and MKDM8ST500IO-O2FA; Firmware Version: 05.M54 / 05.M54BO, 05.M54 / 05.M54CO, 05.M54 / 05.M54DO, 05.M54 / 05.M54FP, 05.M54 / 05.P54DS, 05.M54 / 05.P54FT and 05.M54 / 05.M54CR |