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

June 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: 2024.07.04 11:45:01 -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: 2024.07.03 17:20:20-04'00'
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
4701	06/04/2024	Micron 7400 SSD Controller Sub Chip Security Subsystem	Micron Technology, Inc.	Hardware Version: SCCS v1.0; Firmware Version: Runtime SCSS v2.3; Bootloader v1.0; Function ROM v2.0; Boot ROM v1.0
4702	06/04/2024	Trusted Platform Module ST33KTPM2XSPI / ST33KTPM2XI2C	STMicroelectronics	Hardware Version: P/Ns ST33KTPM2XSPI, ST33KTPM2XI2C ; Firmware Version: 9.256
4703	06/06/2024	Marvell LS2 HSM Family	Marvell Semiconductor, Inc.	Hardware Version: LS2-G-A100-B0; LS2-G-A200-B0; LS2-G-A300-B0; LS2-G-A400-B0; Firmware Version: MARVELL-LS2-FW-10.02-1102, MARVELL-LS2-UBOOT-10.01-10; MARVELL-LS2-FW-10.02-1102, MARVELL-LS2-UBOOT-10.02-1200
4704	06/07/2024	Palo Alto Networks SD-WAN Instant-On Network (ION) Devices ION 1200 and ION 9000	Palo Alto Networks, Inc.	Hardware Version: [ION 1200, ION 1200-C-NA, ION 1200-C-ROW, and ION 1200-C-5G-WW] with FIPS Kit (P/N 920-000363), and ION 9000 with FIPS Kit (P/N 920-000311); Firmware Version: 5.6.3
4705	06/07/2024	PAN-OS 10.1 VM-Series	Palo Alto Networks, Inc.	Software Version: 10.1.5
4706	06/10/2024	OpenSSL FIPS Provider	Think Freely Consulting Incorporated	Software Version: 3.0.8, 3.0.9
4707	06/11/2024	SQLCipher Cryptographic Module (Mobile)	Zetetic, LLC	Software Version: 2.1.2
4708	06/11/2024	SQLCipher Cryptographic Module	Zetetic, LLC	Software Version: 2.1.2
4709	06/13/2024	Samsung NVMe TCG Opal SSC SEDs PM1733a/PM1735a Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLR1T9HCJR-00AC9 [1, 3], MZWLR3T8HCLS-00AC9 [1, 3], MZWLR7T6HBLA-00AC9 [1, 3], MZWLR15THBLA-00AC9 [1, 3], MZWLR30THBLA-00AC9 [1, 3], MZWLR1T9HCJR-00AD9 [2, 4, 6], MZWLR3T8HCLS-00AD9 [2, 4, 6], MZWLR7T6HBLA-00AD9 [2, 4, 6], MZWLR15THBLA-00AD9 [2, 4, 6], MZWLR30THBLA-00AD9 [6], MZWLR1T6HCJR-00AD9 [2, 4, 6], MZWLR3T2HCLS-00AD9 [2, 4, 6], MZWLR6T4HBLA-00AD9 [2, 4, 6], MZWLR12THBLA-00AD9 [2, 4, 6], MZWLR3T8HCLS-00AG6 [5], MZWLR3T8HCLS-00AV8 [5], MZWLR15THBLA-00AG6 [5]; Firmware Version: MPP92E5Q [1], MPP90D3Q [2], MPP95E5Q [3], MPP92D3Q [4], NA50 [5], MPP93D3Q [6]
4710	06/17/2024	Firepower Management Center Virtual VMware Cryptographic Module	Cisco Systems, Inc.	Software Version: 7.0.5
4711	06/17/2024	Firepower Threat Defense Virtual Cryptographic Module	Cisco Systems, Inc.	Software Version: 7.0.5
4712	06/28/2024	Adaptive Security Appliance Virtual Cryptographic Module	Cisco Systems, Inc.	Software Version: 9.16.4

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4713	06/28/2024	Utility Associates Cryptographic Module	Utility Associates, Inc	Software Version: 2.1.2
4714	06/28/2024	Informatica Crypto Platform (ICP) Library	Informatica	Software Version: 2.1.2