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

February 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: 2023.03.06 14:34:27 -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: 2023.03.06 09:26:15-05'00' Foxit PDF Editor Version: 12.1.0

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
4431	02/02/2023	Gen 2 TRANSEC	Comtech Satellite Network Technologies, Inc.	Hardware Version: PL-0023315, Rev A; Firmware Version: 1.1.1
4432	02/06/2023	IBM® Security QRadar® SIEM Cryptographic Module	IBM Corporation	Software Version: 7.4.3
4433	02/09/2023	EZPES Centralized Security Module (CSM)	EasyPost	Hardware Version: CryptoServer CSe-Series 4.00.5.1; Firmware Version: CryptoServer CSe-Series 4.32.0.5; App version: 3.0.0.0
4434	02/15/2023	Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20211004
4435	02/15/2023	Tera2 PCoIP Zero Client Processors	Teradici Corporation	Hardware Version: TERA2140 (Part No. K4B1G1646G-BCH9 and MX29GL256ELT2I-90Q); TERA2321 (Part No. K4B2G1646B-HCH9 and MX25L25635EMI-12G); Firmware Version: 21.01.5-FIPS
4436	02/15/2023	SK hynix PE8010 and PE8030 NVMe Opal SEDs	SK hynix Inc.	Hardware Version: P/Ns HFS960GECTX098N, HFS1T9GECTX098N, HFS3T8GECTX098N, HFS7T6GECTX098N, HFS800GECTX098N, HFS1T6GECTX098N, HFS3T2GECTX098N and HFS6T4GECTX098N; Firmware Version: 11080A10
4437	02/15/2023	SK hynix PE8110 M.2 22110D NVMe TCG Opal SSC SED	SK hynix Inc.	Hardware Version: P/Ns HFS960GDE0X098N, HFS1T9GDE0X098N and HFS3T8GDE0X098N; Firmware Version: 41081A10
4438	02/15/2023	Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20210628
4439	02/15/2023	Skyhigh Security OpenSSL Module	Skyhigh Security	Software Version: 1.1.1v
4440	02/21/2023	VirtruCrypto - FIPS JavaScript Module	Virtru Corporation	Software Version: 1.2.0
4441	02/22/2023	DocuSign QSCD Appliance	DocuSign Ltd.	Hardware Version: 2.0.0.0; Firmware Version: 1.1.0.9
4442	02/23/2023	VMware's ESXboot Cryptographic Module	VMware, Inc.	Software Version: 1.0
4443	02/23/2023	FortiOS 6.4/7.0	Fortinet, Inc.	Firmware Version: FortiOS 6.4 (FIPS-CC-64-5) and FortiOS 7.0 (FIPS-CC-70-6)
4444	02/27/2023	BoringCrypto SoC	Google, LLC.	Software Version: 853ca1ea1168dff08011e5d42d94609cc0ca2e27
4445	02/27/2023	Look-aside Cryptography and Compression Engine (LCE)	Google, LLC	Hardware Version: 3.0; Firmware Version: B0.4.1 FW 6023