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

November 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: GAVIN O'BRIEN Digitally signed by GAVIN O'BRIEN Date: 2023.12.12 11:13:40 -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: 2023.12.11 18:09:49-05'00' 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
4650	11/01/2023	KIOXIA FIPS TC58NC1132GTC Crypto Sub-Chip	KIOXIA Corporation	Software Version: N/A; Hardware Version: 0001; Firmware Version: SC02AS
4651	11/02/2023	Cisco ISR 4000 Series Routers with MACSEC	Cisco Systems, Inc.	Hardware Version: ISR 4321, ISR 4331, ISR 4351 and ISR 4451 with NIM-2GE-CU-SFP; Firmware Version: Cisco IOS-XE 16.12
4652	11/06/2023	Cr50 U2F Cryptographic Library	Google, LLC	Hardware Version: H1B2P; Firmware Version: 1.0.1
4653	11/08/2023	Juniper FIPS Provider	Juniper Networks Inc.	Software Version: 3.0.8
4654	11/14/2023	Ciena 3926 Platform	Ciena Corporation	Hardware Version: 3926; Firmware Version: Ciena Service Aware Operating System (SAOS 10.7.0)
4655	11/22/2023	Qualcomm(R) Pseudo Random Number Generator	Qualcomm Technologies, Inc.	Hardware Version: 2.1.0[1], 2.3.1[2] and 2.4.0[3]
4656	11/27/2023	Cohesity FIPS Object Module	Cohesity, Inc.	Software Version: 2.2.1
4657	11/27/2023	Quantum Cryptographic Module	Quantum Corporation	Software Version: 2.2.1
4658	11/27/2023	Fujitsu Enterprise Postgres Cryptographic Module	Fujitsu Limited	Software Version: 2.2.1
4659	11/27/2023	ClioConnect Cryptographic Module	Altus, Inc.	Software Version: 2.2.1
4660	11/28/2023	CryptoComply for Java	SafeLogic, Inc.	Software Version: 3.1
4661	11/28/2023	Juniper Networks EX4650, QFX5120 and QFX5210 Ethernet Switches	Juniper Networks, Inc	Hardware Version: EX4650-48Y-AFI, EX4650-48Y-AFO, EX4650-48Y-DC-AFI, EX4650-48Y-DC-AFO, QFX5120-32C-AFI , QFX5120-32C-AFO , QFX5120-32C-DC-AFI , QFX5120-32C-DC-AFO, QFX5120-48T-AFI, QFX5120-48T-AFO, QFX5120-48T-DC-AFI, QFX5120-48T-DC-AFO, QFX5120-48Y-AFI2, QFX5120-48Y-AFO2 , QFX5120-48Y-DC-AFI2, QFX5120-48Y-DC-AFO2, QFX5210- 64C-AFI , QFX5210- 64C-AFO, QFX5210-64C-DC-AFI, QFX5210-64C-DC-AFO; Firmware Version: JUNOS OS 20.2R1-S1
4662	11/28/2023	Juniper Networks EX4650, QFX5120 and QFX5210 Ethernet Switches	Juniper Networks, Inc	Hardware Version: EX4650-48Y-AFI, EX4650-48Y-AFO, EX4650-48Y-DC-AFI, EX4650-48Y-DC-AFO, QFX5120-32C-AFI, QFX5120-32C-AFO, QFX5120-32C-DC-AFI, QFX5120-32C-DC-AFO, QFX5120-48Y-AFI2, QFX5120-48Y-AFO2, QFX5120-48Y-DC-AFI2, QFX5120-48Y-DC-AFO2, QFX5210-64C-AFI, QFX5210-64C-AFO, QFX5210-64C-DC-AFI and QFX5210-64C-DC-AFO; Firmware Version: Junos OS 19.3R1
4663	11/28/2023	Juniper Networks SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX5400, SRX5600 and SRX5800 Services Gateways	Juniper Networks, Inc	Hardware Version: [SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX5400, SRX5600 and SRX5800] with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS OS 19.2R1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4664	11/28/2023	Juniper Networks SRX1500, SRX4100, SRX4200 and SRX4600 Services Gateways	Juniper Networks, Inc	Hardware Version: [SRX1500 SYS-JB-AC, SRX1500 SYS-JB-DC, SRX4100 SYS-JB-AC, SRX4100 SYS-JB-DC, SRX4200 SYS-JB-AC, SRX4200 SYS-JB-DC, SRX4600 (AC), SRX4600 (DC)] with JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS OS 19.2R1
4665	11/28/2023	Infinera Groove G30 DCI Platform	Infinera Corporation	Hardware Version: GQS-G30CHASF-00 with tamper-evident labels 550-1211-001; Firmware Version: FP4.3
4666	11/29/2023	Qualcomm(R) Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.6.0
4667	11/30/2023	Datastax BoringCrypto Module	DataStax, Inc.	Software Version: 853ca1ea1168dff08011e5d42d94609cc0ca2e27