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

FIPS VALIDATED 140-2 TM

September 2022

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

Dated:

Digitally signed by
TIMOTHY HALL
Date: 2022.10.12
07:40:12 -04'00'

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall

Dated:

Digitally signed by King, Lyall
DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall"
Reason: I am approving this document
Location: your signing location here
Date: 2022.10.11 11:46:49-04'00'
Foxit PDF Editor Version: 11.2.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4291	09/01/2022	Extreme Networks SLX 9540 and SLX 9740 Switches	Extreme Networks, Inc.	Hardware Version: P/Ns SLX9740-90C, SLX9740-80C, BR-SLX-9540-24S-AC-F, BR-SLX-9540-24S-DC-F, BR-SLX-9540-24S-AC-R, BR-SLX-9540-24S-DC-R, BR-SLX-9540-48S-AC-F, BR-SLX-9540-48S-DC-F, BR-SLX-9540-48S-AC-R and BR-SLX-9540-48S-DC-R; Firmware Version: SLXOS 20.2.1aa
4292	09/06/2022	Ubuntu 20.04 OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 3.1
4293	09/06/2022	Qualcomm(R) Secure Processing Unit	Qualcomm Technologies, Inc.	Hardware Version: 4.1; Firmware Version: spss.a1.1.5_00039
4294	09/10/2022	DIGISTOR® C Series Advanced SSD and Seagate® BarraCudaTM 515 SSD	DIGISTOR	Hardware Version: DIG-M2N22566-AI, DIG-M2N25126-AI, DIG-M2N210006-AI, DIG-M2N220006-AI, ZP256MC30012, ZP512MC30012, ZP1024MC30012, ZP2048MC30012, ZP256MC30022, ZP512MC30022, ZP1024MC30022 and ZP2048MC30022; Firmware Version: ECPM13.1
4295	09/10/2022	Kanguru Defender SED300	Kanguru Solutions	Hardware Version: KSED300-S25-128G-V01 [1], KSED300-S25-256G-V01 [1], KSED300-S25-512G-V01 [1], KSED300-S25-1T-V01 [1], KSED300-S25-2T-V01 [1], KSED300-S2280-128G-V01 [1], KSED300-S2280-256G-V01 [1], KSED300-S2280-512G-V01 [1], KSED300-S2280-1T-V01 [1], KSED300-S2280-2T-V01 [1], KSED300-N2280-256G-V01 [2,3], KSED300-N2280-512G-V01 [2,3], KSED300-N2280-1T-V01 [2,3], KSED300-N2280-2T-V01 [2,3]; Firmware Version: SCPM13.0 [1], ECPM13.0 [2], ECPM13.1 [3]
4296	09/11/2022	AN/GRC-262	Ultra Electronics TCS Inc.	Hardware Version: AN/GRC-262(V)1 with FIPS kit 612-990309-088; Firmware Version: 1.13.10.1336
4297	09/12/2022	NetApp Cryptographic Security Module	NetApp, Inc.	Software Version: 2.0
4298	09/12/2022	Mocana Cryptographic Loadable Kernel Module	DigiCert, Inc.	Software Version: 6.5.2f
4299	09/12/2022	Mocana Cryptographic Suite B Module	DigiCert, Inc.	Software Version: 6.5.2f
4300	09/12/2022	LogRhythm 7.8.0 AI Engine Server	LogRhythm	Software Version: 7.8.0
4301	09/15/2022	Motorola BoringCrypto Android	Motorola Mobility Inc	Software Version: dcdc7bbc6e59ac0123407a9dc4d1f43dd0d117cd
4302	09/19/2022	VaultIC™ 405 1.2.6	WISeKey Semiconductors	Hardware Version: AT90SO72 rev C; Firmware Version: 1.02.6F
4303	09/19/2022	VaultIC™ 405 1.2.6	WISeKey Semiconductors	Hardware Version: AT90SO72 rev C; Firmware Version: 1.02.6F

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4304	09/19/2022	Trusted Platform Module ST33TPHF2XSPI [A], ST33TPHF2XI2C [B], ST33GTPMASPI [C], ST33GTPMAI2C [D], ST33GTPMISPI [E] & ST33GTPMII2C [F]	STMicroelectronics	Hardware Version: ST33HTPH revision A [A [1, 2]], ST33HTPH revision A [B [3]], ST33G1M2A revision F [C [4] and E [4]] and ST33G1M2A revision F [D [5] and F [5]]; Firmware Version: 00.01.02.00 [1], 00.01.03.00 [2], 00.02.02.00 [3], 00.03.02.00 [4] and 00.06.02.00 [5]
4305	09/19/2022	RSA BSAFE(R) Crypto-C Micro Edition	Dell Australia Pty Limited, BSAFE Product Team	Software Version: 4.1.5
4306	09/19/2022	RSA BSAFE(R) Crypto-C Micro Edition	Dell Australia Pty Limited, BSAFE Product Team	Software Version: 4.1.5
4307	09/20/2022	Cocoon Data Content Crypto Service	Cocoon Data	Software Version: 1.0.2.1 [1], 1.0.2.2 [2] and 1.0.2.3 [3]
4308	09/20/2022	Kiteworks Cryptographic Module	Accellion USA, LLC	Software Version: 1.0
4309	09/26/2022	Ultrastar® DC SN640 NVMe™ PCIe 3.0 Self-Encrypting Drive	Western Digital Technologies, Inc.	Hardware Version: P/N WUS4AB0A1D9ELE8; Firmware Version: R501000Q
4310	09/26/2022	iboss Cryptographic Module	iboss Inc.	Software Version: 2.2.1
4311	09/26/2022	CGI Momentum(TM) Java Cryptographic Module	CGI Federal Inc.	Software Version: 3.0.2.1