FIPS 140-2 Consolidated Validation Certificate

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

FIPS VALIDATED 140-2 TM

The Canadian Centre for Cyber Security

June 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

Digitally signed by TIMOTHY HALL
Date: 2022.07.07 08:35:12 -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 with my legally binding signature
Location: your signing location here
Date: 2022.07.05 16:20:32-04'00'
Foxit PDF Editor Version: 11.2.1

Dated:

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
4240	06/01/2022	CryptoComply for Java	SafeLogic Inc,	Software Version: 3.0.2
4241	06/05/2022	SX-590-1402	silex technology, Inc.	Hardware Version: SX-590-1402 01A and SD-330AC-1402 01A; Firmware Version: 2.02
4242	06/06/2022	Huawei EulerOS 2.0 OpenSSH Server Cryptographic Module	Huawei Technologies Co., Ltd.	Software Version: 1.1
4243	06/06/2022	PTP 700 Point to Point Wireless Ethernet Bridge	Cambium Networks, Ltd.	Hardware Version: P/Ns C045070B003A, C045070B003B, C045070B034A, C045070B039A, C045070B044A, C045070B046A, C045070B048A, C045070B004A, C045070B038A, C045070B040A, C045070B045A, C045070B047A, C045070B049A, C070070B001A, C070070B003A, C070070B005A, C070070B007A, C070070B009A, C070070B011A, C070070B002A, C070070B004A, C070070B006A, C070070B008A, C070070B010A, C070070B012A; Firmware Version: 700-03-50-FIPS
4244	06/07/2022	Nexthink Cryptographic library	Nexthink, Inc.	Software Version: 1.0
4245	06/07/2022	Keysight Technologies Cryptographic Module for Network Visibility	Keysight Technologies	Software Version: 1.0.2.1, 1.0.2.2 and 1.0.2.3
4246	06/09/2022	Huawei EulerOS 2.0 OpenSSH Client Cryptographic Module	Huawei Technologies Co., Ltd.	Software Version: 1.1
4248	06/10/2022	Qube Xi Integrated Media Block	Qube Cinema Technologies Pvt. Ltd.	Hardware Version: P/Ns Qube-Xi-IS1 rev.1.1, Qube-Xi-IF1 rev.1.1, Qube-Xi-MS1 rev.1.1 and Qube-Xi-MF1 rev.1.1; Firmware Version: Firmware Version: 1.23.157.20779 or 1.25.176.2721 Bootloader Version: 1.3.7.18217
4249	06/13/2022	Nutanix Cryptographic Module for OpenSSL	Nutanix, Inc.	Software Version: 6.0
4250	06/13/2022	QASM Cryptographic Module	Crypto4A Technologies Inc.	Hardware Version: 1.0; Firmware Version: 2.1.0
4251	06/17/2022	AT-x220, AT-x320, AT-x950 Secure Management Module	Allied Telesis	Hardware Version: P/Ns AT-x220-28GS, 990-007791-F90, [A] [B], AT-x220-52GT, 990-007760-F90, [A] [B], AT-x220-52GP, 990-007758-F90, [A] [B], AT-x320-10GH, 990-007775-F00 with one from [1], [A] [C], AT-x320-11GPT, 990-007774-F90, [A] [C], AT-x950-52XSQ, 990-007713-F00 with two from [2], [A] [D] and AT-x950-52XTQm, 990-007714-F00 with two from [2], [A] [D]; Power Supply Units 990-006217-10 [1] and 990-006195-10 [2]; Firmware Version: 5.5.1.APCERT-0.3.rel [A]; Bootloader: bl-6.2.26-x220-D522-8F27.kwb [B], bl-6.2.26-x320-D76F-8439.kwb [C] and bl-6.2.28-x950-C388-345C.bin [D]
4252	06/21/2022	Aerospike Enterprise Database Federal Edition	Aerospike, Inc.	Software Version: 2.2
4253	06/23/2022	Microsoft BoringCrypto Module	Microsoft Corporation	Software Version: 7f02881e96e51f1873afcf384d02f782b48967ca

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4254	06/23/2022	Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20210302
4255	06/23/2022	Zettaset XCrypt FIPS Cryptographic Library	Zettaset, Inc	Software Version: 1.0.2.1[1], 1.0.2.2 [2] and 1.0.2.3 [3]
4256	06/24/2022	Panasonic BoringCrypto Module	Panasonic Corporation of North America	Software Version: 7f02881e96e51f1873afcf384d02f782b48967ca
4257	06/24/2022	Gloo BoringCrypto	Solo.io	Software Version: 1701
4258	06/27/2022	Macronix ArmorFlash MX78 series	Macronix International Co., Ltd.	Hardware Version: MX78U64A00F, MX78U64B00G, MX78U128A00F, MX78U128B00G, MX78U256A00F, MX78U256B00G, MX78L64A00F, MX78L64B00G, MX78L128A00F, MX78L128B00G, MX78L256A00F, MX78L256B00G
4259	06/29/2022	Barracuda KTINA FIPS Crypto Module	Barracuda Networks	Software Version: 8.0