FIPS 140 Series Consolidated Validation Certificate

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

The Canadian Centre for Cyber Security

August 2024

The National Institute of Standards and Technology, as the United States FIPS 140 Series Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140 Series Cryptographic Module Validation Authority; hereby validate the FIPS 140 Series testing results of the cryptographic modules listed below. The FIPS 140 Series specify 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 the FIPS 140 Series 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.

The FIPS 140 Series 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 the areas of a cryptographic module that are related to its secure design and implementation.

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: 2024.09.06 09:44:08 -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:
Date: 2024.09.06 08:56:00-04'00'
Foxit PDF Editor Version: 13.1.3

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
4747	08/01/2024	Cisco FIPS Object Module	Cisco Systems, Inc.	Firmware Version: 7.3a
4748	08/01/2024	Qualcomm(R) Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.7.0[1], 5.7.2[2] and 5.7.3[3]
4749	08/02/2024	Crypto Module for Intel® Alder Point PCH Converged Security and Manageability Engine (CSME)	Intel Corporation	Hardware Version: 4.6.0.0; Firmware Version: 5.2.0.0
4750	08/02/2024	Kernel Cryptography Module for AlmaLinux 9	Cloudlinux Inc., TuxCare division	Software Version: kernel 5.14.0-284.11.1.el9_2.tuxcare.5 5.14.0-284.11.1.el9_2.tuxcare.6; libkcapi 1.3.1-3.el9
4751	08/05/2024	Nokia 1830 Photonic Service Switch (PSS) R23.3 Nokia 1830 Photonic Service Interconnect – Modular (PSI-M) R23.3	Nokia of America Corporation (Nokia)	Hardware Version: Hardware Version: PSS-8 Chassis (WOMPU00CRA / 3KC48901AA) [1], PSS-16II Chassis (WOMR300BRA / 3KC48960AC) [2], PSS-32 Chassis (WOM4V10GRA / 8DG59319AB) [3], PSS-24x Chassis (WOMP410CRB / 3KC50378AA) [4] and PSI-M Chassis (3KC81791AA) [5]; 8EC2 Card (3KC48820AA) [1], 32EC2 Card (8DG63979AA) [2, 3], CEC2 Card (3KC50335AA) [4] and MEC2 Card (3KC81775AA) [5]; 11QPEN4 (8DG60996AA) [1-3], S13X100E (8DG63988AA) [1-3], 2UC400E (3KC60522AA) [4], DFC12E (3KC82081AA) [5] and 8P20 (3KC49240AA) [1-3]; MFC24X Multi-Function Card (3KC50330AA) [4]; Filler Card (8DG59418AA) [1-3], Filler Card (3KC59819AC) [4] and Filler Card (3KC81780AA) [5]; Security Label Kit (8DG-6509-AAAA) [1-5]; ; Firmware Version: 1830PSS ECN R23.3, 1830PSI-M ECN R23.3
4752	08/07/2024	IOS Common Cryptographic Module (IC2M)	Cisco Systems, Inc.	Firmware Version: Rel5b
4753	08/08/2024	CorSSL FIPS Object Module	Corsec Security, Inc.	Software Version: 2.0.16.001
4754	08/09/2024	Red Hat Enterprise Linux 9 libgcrypt	Red Hat(R), Inc.	Software Version: 1.10.0-8b6840b590cedd43
4755	08/09/2024	IBM® Crypto for C	IBM Corporation	Software Version: 8.8.1.0
4756	08/09/2024	Apple corecrypto Module v11.1 [Apple silicon, Secure Key Store, Hardware] (SL2)	Apple Inc.	Hardware Version: 2.0; Firmware Version: 11.1
4757	08/09/2024	Apple corecrypto Module v11.1 [Apple silicon, Secure Key Store, Hardware, SL2/PHY3]	Apple Inc.	Hardware Version: 2.0; Firmware Version: 11.1
4758	08/12/2024	CryptoManager Root of Trust RT-660	Rambus Inc.	Hardware Version: 0x6000_0931; Firmware Version: 2022-02-24-g801c166
4759	08/14/2024	AWS-LC Cryptographic Module (dynamic)	Amazon Web Services Inc.	Software Version: AWS-LC FIPS 2.0.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4760	08/14/2024	PAN-OS 10.2 running on PA-220, PA-220R, PA-400 Series, PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, and PA-7000 Series NGFWs	Palo Alto Networks, Inc.	Hardware Version: 910-000102 with Physical Kit 920-000112, 910-000122 with Physical Kit 920-000119, 910-000128 with Physical Kit 920-000084, 910-000147 with Physical Kit 920-000226, 910-000223 with Physical Kit 920-000309, [910-000119 and 910-000120] with Physical Kit 920-000185, [910-000125, 910-000131, 910-000132, and 910-000157] with Physical Kit 920-000186, [910-000162, 910-000163, and 910-000164] with Physical Kit 920-000212, [910-000212, 910-000230, 910-000231, and 910-000232] with Physical Kit 920-000454, [910-000241, 910-000242, 910-000243, and 910-000244] with Physical Kit 920-000333, and , [910-000252, 910-000253, and 910-000254] with Physical Kit 920-000320; Firmware Version: 10.2.8-h4
4761	08/14/2024	Mocana Cryptographic Suite B Module	DigiCert, Inc.	Software Version: 7.0.0f_u1
4762	08/15/2024	PAN-OS 10.2 VM-Series	Palo Alto Networks, Inc.	Software Version: 10.2.8-h4
4763	08/16/2024	Peplink FIPS Module	Peplink Pepwave Limited	Software Version: 3.0.8
4764	08/16/2024	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.3
4765	08/19/2024	nShield 5s Hardware Security Module	Entrust	Hardware Version: PCA10005-01 revision 03 and 04; Firmware Version: primary-version 13.4.5; recovery-version 13.2.4; uboot-version 1.1.0
4766	08/19/2024	Kernel Mode Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.19042, 10.0.19043, 10.0.20348 and 10.0.22000
4767	08/19/2024	Zebra 8887 Cryptographic Module	Zebra Technologies Corporation	Hardware Version: 9134; Firmware Version: FIPS Driver Firmware Version 2.1; NXP Firmware Version 15.68.19.p59
4768	08/19/2024	Palo Alto Networks SD-WAN Virtual Instant-On Network (vION)	Palo Alto Networks, Inc.	Software Version: 6.1.2
4769	08/20/2024	Gigamon's SL-FJA (SafeLogic FIPS Java API)	Gigamon Inc.	Software Version: 3.0.2.1
4770	08/20/2024	Cradlepoint Cryptographic Module	Cradlepoint, Inc.	Software Version: 1.0
4771	08/20/2024	Toshiba Secure TCG Opal SSC Self-Encrypting Drive Series MG09ACP18TA and MG09ACP16TA	Toshiba Electronic Devices & Storage Corporation	Software Version: N/A; Hardware Version: A0 with MG09ACP18TA and A0 with MG09ACP16TA; Firmware Version: PD82
4772	08/21/2024	IDCore 3230 / 230 Platform	Thales	Hardware Version: SLC37GDA512 (A2848377)[1], SLC37GDA512 (A2848344)[2] and SLC37GDA512 (A3138921)[1]; Firmware Version: [IDCore 230-BUILD6.11, Demonstration Applet version V1.D][1] and [IDCore 3230-BUILD6.11, Demonstration Applet version V1.D][2]
4773	08/21/2024	PAN-OS 11.0 VM-Series	Palo Alto Networks, Inc.	Software Version: 11.0.3-h12

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4774	08/21/2024	Red Hat Enterprise Linux 9 NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: 4.34.0-a20cd33fbbe14357
4777	08/23/2024	Panorama 10.2 M-200, M-300, M-600 and M-700	Palo Alto Networks, Inc.	Hardware Version: 910-000175 with FIPS Kit 920-000209, 910-000176 with FIPS Kit 920-000208, 910-000270 with FIPS Kit 920-000318, 910-000271 with FIPS Kit 920-000319; Firmware Version: 10.2.3-h1
4778	08/25/2024	Qualcomm® Pseudo Random Number Generator	Qualcomm Technologies, Inc.	Hardware Version: 3.1.0; Firmware Version: 7fab7110b4ff04e70460b9ffd9b2b5b96ba33faabbec40cb67c87a14c79f658fdd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d
4779	08/25/2024	Oracle Linux 9 OpenSSL FIPS Provider	Oracle Corporation	Software Version: 3.0.7-b27cdeb3ba51be46
4780	08/26/2024	Red Hat Enterprise Linux 9 gnutls	Red Hat, Inc.	Software Version: 3.7.6-66803fa128d6a6e5
4781	08/27/2024	CryptoComply 140-3 FIPS Provider	SafeLogic Inc.	Software Version: 3.0.0-FIPS 140-3, 3.0.1-FIPS 140-3
4782	08/28/2024	DocuSign QSCD Appliance	DocuSign, Inc.	Hardware Version: 2.0.0.0; Firmware Version: 1.2.0.7
4783	08/29/2024	Panorama Virtual Appliance 10.2	Palo Alto Networks, Inc.	Software Version: 10.2.3-h1
4784	08/29/2024	Wildfire 10.2 WF-500 and WF-500-B	Palo Alto Networks, Inc.	Hardware Version: 910-000097 with FIPS Kit 920-000145, 910-000270 with FIPS Kit 920-000318; Firmware Version: 10.2.3-h1