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

September 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: 2023.10.12 10:41:51 -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 Location: Date: 2023.10.11 11:21:29-04'00' Foxit PDF Editor Version: 12.1.2

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

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4578	09/01/2023	SUSE Rancher Kubernetes Cryptographic Library	SUSE LLC	Software Version: 66005f41fbc3529ffe8d007708756720529da20d
4579	09/01/2023	Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access points, Version 8.10, 16.12	Cisco Systems, Inc.	Hardware Version: 1562e, 1562i, 1562d, 1562ps, 2802e, 2802i, 3802e, 3802i, 3802p and 4800 with FIPS Kit: AIR-AP-FIPSKIT=; Firmware Version: 8.10, 16.12
4580	09/04/2023	HT Satellite Terminal	Hughes Network Systems, LLC	Hardware Version: HT2010; Firmware Version: 7.4.1.19
4581	09/04/2023	HT Satellite Terminals	Hughes Network Systems, LLC	Hardware Version: HT2300; HT2500; HT2550; HT2650; Firmware Version: 7.4.1.19
4582	09/04/2023	PL-2000M, PL-2000AD and PL-2000ADS	PacketLight Networks Ltd.	Hardware Version: PL-2000M, PL-2000AD, PL-2000ADS; Firmware Version: 1.3.12d
4583	09/05/2023	Primus HSM	Securosys SA	Hardware Version: P/Ns E20 / 60-1004 Rev0, E60 / 60-1004 Rev0, E150 / 60-1004 Rev0, EP700 / 60-1008 Rev0, X200 / 60-1002 Rev1, X400 / 60-1002 Rev1, X700 / 60-1002 Rev1 and X1000 / 60-1010 Rev1; Firmware Version: 2.5.14
4584	09/06/2023	Nutanix Cryptographic Module for BoringSSL	Nutanix, Inc.	Software Version: ae223d6138807a13006342edfeef32e813246b39
4585	09/06/2023	Hewlett Packard Enterprise BouncyCastle Module	Hewlett Packard Enterprise Development LP	Software Version: 1.0.2.3
4586	09/06/2023	Oracle Linux 7 NSS Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
4587	09/06/2023	Barracuda OpenSSL FIPS Provider	Barracuda Networks	Software Version: 3.0.8
4588	09/07/2023	SafeZone FIPS Cryptographic Module	Rambus Inc.	Software Version: 1.2.1
4589	09/08/2023	Ubuntu 16.04 OpenSSL Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4590	09/08/2023	TippingPoint Crypto Core OpenSSL	Trend Micro Inc.	Software Version: 1.0.2l-fips
4591	09/11/2023	IBM(R) z/OS(R) Version 2 Release 4 ICSF PKCS #11 Cryptographic Module	IBM Corporation	Software Version: ICSF level HCR77D0 with APAR OA63132; Hardware Version: COP chips integrated within processor unit [1] and COP chips integrated within processor unit and P/N 02WN654-N37880 (Low Power) [2]; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 41C [1], and Feature 3863 (aka FC3863) with System Driver Level 41C and CCA 7.0.68z [2]
4592	09/12/2023	Arista EOS Crypto Module	Arista Networks, Inc.	Software Version: v2.1
4593	09/12/2023	Amazon Linux 2 Kernel Crypto API Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
4594	09/12/2023	Ubuntu 18.04 IBM-GT Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4595	09/12/2023	VMware's IKE Crypto Module	VMware, Inc.	Software Version: 1.1.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4596	09/13/2023	Ubuntu 18.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4597	09/13/2023	Ubuntu 18.04 AWS Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4598	09/13/2023	Ubuntu 18.04 Google Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4599	09/13/2023	Cryptographic Module for Intel® Platforms' Security Engine Chipset	Intel Corporation	Hardware Version: 3.1; Firmware Version: 3.0
4600	09/14/2023	HYCU Cryptographic Library Module	HYCU, Inc.	Software Version: 1.0.2.1, 1.0.2.2 and 1.0.2.3
4601	09/18/2023	RF-7800W Broadband Ethernet Radio	L3Harris Technologies, Inc.	Hardware Version: RF-7800W-OU470, P/N: 12069-3000-01, Hardware P/N: 12069-3035-01, Version C, RF-7800W-OU471, P/N: 12069-3000-04, Hardware P/N: 12069-3035-02, Version C, RF-7800W-OU473, P/N: 12069-3000-08, Hardware P/N: 12069-3035-04, Version -, RF-7800W-OU492, P/N: 12069-3000-07, Hardware P/N: 12069-3035-03, Version C, RF-7800W-OU500, P/N: 12069-3000-03, Hardware P/N: 12069-3035-01, Version C, RF-7800W-OU501, P/N: 12069-3000-06, Hardware P/N: 12069-3035-02, Version C, RF-7800W-OU503, P/N: 12069-3000-09, Hardware P/N: 12069-3035-04, Version -, RF-7800W-RP470, P/N: 12069-5000-01, Hardware P/N: 12069-5010-01, Version C, RF-7800W-RP471, P/N: 12069-5000-02, Hardware P/N: 12069-5010-02, Version C, RF-7800W-RP473, P/N: 12069-5000-04, Hardware P/N: 12069-5010-04, Version C, RF-7800W-RP500, P/N: 12069-5000-21, Hardware P/N: 12069-5010-01, Version C, RF-7800W-RP501, P/N: 12069-5000-22, Hardware P/N: 12069-5010-02, Version C and RF-7800W-RP503, P/N: 12069-5000-24, Hardware P/N: 12069-5010-04, Version C; Firmware Version: 6.20
4602	09/20/2023	Code Integrity	Microsoft Corporation	Software Version: 10.0.17763.10021 and 10.0.17763.10127
4603	09/21/2023	Nuvoton Cryptographic Library 2.0	Nuvoton Technology Corporation	Hardware Version: 2.1.3
4604	09/25/2023	Ubuntu 16.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
4605	09/25/2023	LiveAction Cryptographic Module	LiveAction, Inc.	Software Version: 2.2.1
4606	09/26/2023	Cisco Catalyst 9800 (40/80/L) Wireless Controllers running IOS-XE 16.12	Cisco Systems, Inc.	Hardware Version: 9800-40, 9800-80 and 9800-L; Firmware Version: IOS-XE 16.12
4607	09/26/2023	FortiGate-VM	Fortinet, Inc.	Software Version: FortiGate-VM 6.2, build 5203
4608	09/26/2023	FortiGate-6300F/6301F/6500F/6501F	Fortinet, Inc.	Hardware Version: FortiGate-6300F (C1AG83), FortiGate-6301F (C1AG85), FortiGate-6500F (C1AG84) and FortiGate-6501F (C1AG86) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5204

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4609	09/27/2023	FortiGate-201E/301E/401E/501E/601E	Fortinet, Inc.	Hardware Version: FortiGate-201E (C1AE64), FortiGate-301E (C1AG46), FortiGate-401E (C1AH76), FortiGate-501E (C1AG44) and FortiGate-601E (C1AH71) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5203
4610	09/27/2023	FortiGate-3401E/3601E/3960E/3980E	Fortinet, Inc.	Hardware Version: FortiGate-3401E (C1AH85), FortiGate-3960E (C1AF81), FortiGate-3601E (C1AH57) and FortiGate-3980E (C1AF63) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5203
4611	09/27/2023	FortiGate-61E/61F/81E/101E/101F and FortiWiFi-61E	Fortinet, Inc.	Hardware Version: FortiGate-61E (C1AE14), FortiGate-61F (C1AJ23), FortiGate-81E (C1AE21), FortiGate-101E (C1AE27), FortiGate-101F (C1AJ44) and FortiWiFi-61E (C1AE18) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5203
4612	09/27/2023	FortiGate-600D/1200D/1500D/3000D/3700D and FortiGate-5001D with FortiGate-5144C Chassis	Fortinet, Inc.	Hardware Version: FortiGate-600D (C1AE11), FortiGate-1200D (C1AC57), FortiGate-1500D (C1AA64), FortiGate-3000D (C1AC63), FortiGate-3700D (C1AA92), FortiGate-5001D (C1AA92), FortiGate-5144C (C1AB98), Blank Filler Panel - Front (P16708-01) and Blank Filler Panel - Rear (P16710-01) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5203
4613	09/27/2023	FortiGate-5001E1 Blade with FortiGate-5144C Chassis	Fortinet, Inc.	Hardware Version: FortiGate-5001E1 (C1AG76), FortiGate-5144C (C1AB98), Blank Filler Panel - Front (P16708-01), Blank Filler Panel - Rear (P16710-01) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5203
4614	09/27/2023	FortiOS 6.2	Fortinet, Inc.	Firmware Version: FortiOS 6.2 build 5203
4615	09/27/2023	Acronis SCS Cryptographic Module	Acronis SCS	Software Version: 1.0
4616	09/27/2023	BC-FJA (Bouncy Castle FIPS Java API)	Legion of the Bouncy Castle Inc.	Software Version: 1.0.2.1 [1], 1.0.2.2 [2], 1.0.2.3 [3] and 1.0.2.4 [4]
4617	09/28/2023	Hewlett Packard Enterprise OpenSSL Cryptographic Module on Ubuntu Linux	Aruba, a Hewlett Packard Enterprise company	Software Version: 2.1
4618	09/28/2023	IBM(R) z/OS(R) Version 2 Release 4 System SSL Cryptographic Module	IBM Corporation	Software Version: HCPT440/JCPT441 with APAR OA59268; Hardware Version: COP chips integrated within processor unit; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 41C
4619	09/28/2023	OpenSSL FIPS Provider	BAE Systems Information and Electronics Systems Integration, Inc.	Software Version: 3.0.8
4620	09/29/2023	Xage Cryptographic Module for OpenSSL	Xage Security, Inc.	Software Version: 3.0.8