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

August 2021

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: 2021.09.13 15:05:37 -04'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Sproule, Lisa Digitally signed by Sproule, Lisa DN: C=CA, O=GC, OU=CSE-CST, CN="Sproule, Lisa" Reason: I am the author of this document Location: your signing location here Date: 2021.09.10 11:48:49-04'00' Foxit PDF Editor Version: 11.0.1

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
3997	08/03/2021	Network Security Platform Sensor NS7500	McAfee, LLC	Hardware Version: P/N IPS-NS7500 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.15
3998	08/03/2021	CareView Cryptographic Module	CareView Communications, Inc.	Software Version: 1.0
3999	08/03/2021	Philips FIPS Object Module for OpenSSL	Koninklijke Philips N.V.	Software Version: 1.0
4000	08/03/2021	Cohesity FIPS Object Module for OpenSSL	Cohesity Inc.	Software Version: 1.0
4001	08/03/2021	ControlUp OpenSSL FIPS library	ControlUp Technologies, Inc	Software Version: 1.0
4002	08/03/2021	Tanium FIPS OpenSSL Module	Tanium, Inc.	Software Version: 1.0
4003	08/03/2021	OTP Token	FEITIAN Technologies	Hardware Version: P449, V1.0; Firmware Version: V1.0 (build015010, build015210, build021010 or build021210)
4004	08/03/2021	Dynatrace Java Crypto Module	Dynatrace, Inc.	Software Version: 1.0.2.1
4005	08/06/2021	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], KSED300-N2280-512G-V01 [2], KSED300-N2280-1T-V01 [2], KSED300-N2280-2T-V01 [2]; Firmware Version: SCPM13.0 [1], ECPM13.0 [2]
4006	08/10/2021	FireEye NX Series: NX1500V, NX2500V, NX2550V, NX4500V, NX6500V	FireEye, Inc.	Software Version: 9.0.3
4007	08/11/2021	IBM(R) z/VM(R) Version 7 Release 2 System SSL Cryptographic Module	IBM Corporation	Software Version: 5735FAL00: z/VM Version 7 Release 2 with 7201RSU (GA-level release) and the PTF for APAR PH24751; Hardware Version: z14 CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863
4008	08/11/2021	K350	DataLocker Inc.	Hardware Version: SK350-016, SK350-064, SK350-256; Firmware Version: Firmware Version 1.48 and Bootloader Version 1.03

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4009	08/12/2021	FIPS SE051	NXP Semiconductors	Hardware Version: FIPS SE051 Full [SE050 (N7121 B1)] [1, 2] and FIPS SE051 Reduced [SE050 (N7121 B1)] [3]; Firmware Version: [Platform ID 4A335233353130323942343131313030 4C0954E73E773C6E and ROM ID 2E5AD88409C9BADB and Patch ID 1 and NXP SEMS Lite applet v1.4.0.11 and NXP IoT applet v6.0.0] [1], [Platform ID 4A335233353130323942343131313030 4C0954E73E773C6E and ROM ID 2E5AD88409C9BADB and Patch ID 1 and NXP SEMS Lite applet v1.4.0.11] [2] and [Platform ID 4A335233353130323942343131313030 1A08FA5067B5F256 and ROM ID 2E5AD88409C9BADB and Patch ID 1 and NXP SEMS Lite applet v1.4.0.11 and NXP IoT applet v6.0.0] [3]
4010	08/19/2021	Ultrastar® He¹² and Ultrastar® DC HC520 TCG Enterprise HDD	Western Digital Corporation	Hardware Version: P/Ns HUH721212AL5205 (1) [1, 2, 3, 4, 5], HUH721212AL5205 (2) [1, 2, 3, 4, 5], HUH721212AL4205 (1) [1], HUH721212AL4205 (2) [1]; Firmware Version: R925 [1], R92C [2], R9C0 [3], NM08 [4], NM09 [5]
4011	08/19/2021	Ultrastar® He¹° and Ultrastar® DC HC510 TCG Enterprise HDD	Western Digital Corporation	Hardware Version: P/Ns HUH721010AL5205 (1) [1, 2, 3], HUH721010AL5205 (2) [1, 2, 3], HUH721010AL4205 (1) [1], HUH721010AL4205 (2) [1], HUH721008AL5205 (1) [1, 2, 3], HUH721008AL5205 (2) [1, 2, 3], HUH721008AL4205 (1) [1], HUH721008AL4205 (2) [1]; Firmware Version: R92C [1], R9C0 [2], LM09 [3]
4012	08/19/2021	GlobalProtect App	Palo Alto Networks, Inc.	Software Version: 5.1.4
4013	08/24/2021	iStorage datAshur BT	iStorage Ltd.	Hardware Version: IS-FL-DBT-256-4, IS-FL-DBT-256-8, IS-FL-DBT-256-16, IS-FL-DBT-256-32, IS-FL-DBT-256-64, IS-FL-DBT-256-128; Firmware Version: V1.01.10 and V2.4
4014	08/24/2021	MFP Cryptographic Module(A)	Kyocera Document Solutions Inc.	Hardware Version: VaultIP-2.1.10 and EIP38-3.2; Firmware Version: 2.2.18
4015	08/24/2021	Verizon OpenSSL Library	Verizon	Software Version: 1.0
4016	08/24/2021	codeEncrypt	Code Corporation	Software Version: 4.5.2
4017	08/27/2021	Taglio PIV Applet v2.1 on NXP JCOP 3 SecID P60 CS (OSB)	Taglio	Hardware Version: P6022y VB; Firmware Version: 19790400
4018	08/30/2021	Ubuntu 18.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.1
4019	08/30/2021	Arista EOS Crypto Module	Arista Networks, Inc.	Software Version: v2.0
4020	08/30/2021	Ruckus Networks SmartZone 144 (SZ-144) and SmartZone 300 (SZ-300) WLAN Controllers	CommScope Technologies LLC	Hardware Version: PF1-S144-US00, RevA; PF1-S300-WW00, RevA; PF1-S300-WW10, RevA; Firmware Version: 5.2.1.3
4021	08/31/2021	PESA Crypto Module	PESA, Inc.	Software Version: 1.0