FIPS 140-2 Consolidated Validation Certificate

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

The Communications Security Establishment of the Government of Canada

October 2018

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, 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: Michael J Cooper
Dated: 11/5/2018
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature:
Dated: 2018-11-07
Director, Security Architecture and Risk Management
Communications Security Establishment

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
3195	10/15/2018	Code Integrity	Microsoft Corporation	Software Version: 10.0.15063.674 [1], 10.0.15254 [2] and 10.0.16299 [3]
3197	10/22/2018	Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.15063.674 [1], 10.0.15254 [2] and 10.0.16299 [3]
3298	10/15/2018	NuixCrypt	Nuix USG Inc.	Software Version: 3.14.2
3299	10/15/2018	FastIron ICX™ 7450 Series Switch/Router	Ruckus Wireless, Inc.	Hardware Version: ICX7450-24P, ICX7450-48P, ICX7450-48F, ICX7400-4X1GF, ICX7400-4X10GF, ICX7400-4X10GC, ICX7400-1X40GQ, ICX7400-SERVICE-MOD, RPS16-E, RPS16DC-E, RPS16-I, RPS16DC-I, ICX-FAN10-I, ICX-FAN10-E, Filler Panel; Firmware Version: IronWare R08.0.70
3300	10/15/2018	Windows Embedded Compact Cryptographic Primitives Library (bcrypt.dll)	Microsoft Corporation	Software Version: 7.00.2883
3301	10/15/2018	SafeNet PCIe Cryptographic Module for SafeNet IS	Gemalto	Hardware Version: VBD-05-0101; VBD-05-0102; and VBD-05-0103; Firmware Version: 6.3.4
3302	10/15/2018	Trusted Platform Module ST33TPHF2ESPI & ST33TPHF2EI2C	STMicroelectronics	Hardware Version: ST33HTPH2E28AAF0 [1], ST33HTPH2E32AAF0 [1], ST33HTPH2E28AAF1 [1], ST33HTPH2E32AAF1 [1], ST33HTPH2E28AHB3 [1], ST33HTPH2E32AHB3 [1], ST33HTPH2E28AHB4 [1], ST33HTPH2E32AHB4 [1], ST33HTPH2E28AHB7 [2], ST33HTPH2E32AHB7 [2], ST33HTPH2E28AHB8 [2], ST33HTPH2E32AHB8 [2], ST33HTPH2E28AHC0 [1], ST33HTPH2E32AHC0 [1], ST33HTPH2E28AHC2 [2] and ST33HTPH2E32AHC2 [2]; Firmware Version: 49.08 [1] and 49.09 [2]
3303	10/17/2018	HPE SimpliVity OmniStack Crypto Library	Hewlett Packard Enterprise Development LP	Software Version: 2.1
3304	10/17/2018	Docker Enterprise Edition Crypto Library	Docker, Inc.	Software Version: 1.0
3305	10/18/2018	128 Technology Cryptographic Module	128 Technology	Software Version: 2.2
3306	10/19/2018	Cisco FTD FX-OS on 4K/9K Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR4110-ASA-K9[1], FPR4120-ASA-K9[1], FRP4140-ASA-K9[1], FRP4150-ASA-K9[1], FPR9K-SM24 (SM-24)[2], FPR9K-SM36 (SM-36)[2] and FPR9K-SM44 (SM-44)[2] with FIPS Kit (Cisco_TEL.FIPS_Kit), and opacity shield 69-100250-01[1] or 800-102843-01[2]; Firmware Version: 2.2
3307	10/19/2018	Samsung NVMe TCG Opal SSC SEDs PM1723b Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLL3T8HAJQ-000G6; Firmware Version: NA00
3308	10/19/2018	StarSign PIV Applet V 1.0 on Giesecke+Devrient Sm@rtCafé Expert 7.0	Giesecke+Devrient Mobile Security GmbH	Hardware Version: SLE78CLFX4000P (M7892); Firmware Version: Sm@rtCafé Expert 7.0, StarSign PIV Applet V1.0
3309	10/19/2018	CryptoComply	SafeLogic, Inc.	Software Version: 3.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3310	10/23/2018	IDCore 3130 Platform	Gemalto	Hardware Version: P/Ns SLE78CLFX400VPH and SLE78CFX400VPH with packaging options A1977038, A1714221 and A2023188; Firmware Version: IDCore 3130 (Build09C), Demonstration Applet version V1.6
3311	10/23/2018	Ixia Cryptographic Module for Java	Ixia, a Keysight Business	Software Version: 1.0.1
3312	10/23/2018	TI SimpleLink WiFi Networking Subsystem Crypto Module	Texas Instruments, Inc.	Hardware Version: Chip ID 0x311001; Firmware Version: 4.1.0.16
3313	10/23/2018	Ixia Cryptographic Module for OpenSSL	Ixia, a Keysight Business	Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16
3314	10/23/2018	Hitachi Flash Module Drive HDE	Hitachi, Ltd.	Hardware Version: P/N: 3286810-A or 3286811-A; Version: A; Firmware Version: J0J0
3315	10/26/2018	Cisco Firepower Threat Defense on ASA Cryptographic Module	Cisco Systems, Inc.	Hardware Version: ASA 5506-X[1][2], ASA 5506H-X[1][2], ASA 5506W-X[1][2], ASA 5508-X[1][3], ASA 5516-X[1][4], ASA 5525-X[1], ASA 5545-X[1] and ASA 5555-X[1] with [AIR-AP-FIPSKIT=][1], [ASA5506-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3] and [ASA5516-FIPS-KIT=][4]; Firmware Version: 6.2
3316	10/31/2018	Seagate Secure(R) TCG Enterprise SSC Self-Encrypting Drive	Seagate Technology, LLC	Hardware Version: XS1600ME10023, XS800ME10023, XS400ME10023, XS1600LE10023, XS1920SE10123, XS3840TE10023, XS3200ME70023, XS7680TE70023, XS6400LE70023; Firmware Version: 7A51