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

August 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: 10/1/2018
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature:
Dated: 13/9/2018
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
3252	08/01/2018	Seagate Secure(R) TCG Opal SSC Self-Encrypting Drive (SED) FIPS 140-2 Module	Seagate Technology LLC	Hardware Version: ST500LM033 - 1RD17D[1], ST1000LM038 - 1RD172[2], ST2000LM010 - 1RA174[3], ST1000LX017 - 1U9172[4], ST2000LX003 - 1RJ174[5], ST500LM035 - 2GJ17A[6], ST1000LM050 - 2GJ172[7]; Firmware Version: SDM1[1,2,3,6,7], SDM2[1,2,3,6,7], RSE1[1,2], LSM1[1,2,3], RDE1[3], SSM1[4,5], RSE2[1,2], RSE3[1,2], RDE2[3], RDE3[3], RXE1[6,7], RXE3[6,7], LXM7[6,7]
3253	08/02/2018	iStorage FIPS 140-2 Level 3 Module Rev 1.0	iStorage Ltd.	Hardware Version: Rev 1.0; Firmware Version: EC Firmware version IS_EC_FW_2_59_1X and SC Firmware version 3.1
3254	08/02/2018	NITROXIII CNN35XX-NFBE HSM Family	Cavium Inc.	Hardware Version: P/Ns CNL3560P-NFBE-G, CNL3560-NFBE-G, CNL3530-NFBE-G, CNL3510-NFBE-G, CNL3510P-NFBE-G, CNN3560P-NFBE-G, CNN3560-NFBE-G, CNN3530-NFBE-G and CNN3510-NFBE-G; Firmware Version: CNN35XX-NFBE-FW-2.04 build 17
3255	08/02/2018	Samsung Flash Memory Protector V1.4	Samsung Electronics Co., Ltd.	Software Version: 1.4; Hardware Version: 4.0
3256	08/09/2018	7705 SAR-OS SAR-18/8/X/Ax/Wx/W/H/Hc Data Plane Cryptographic Module (SARDPCM)	Nokia Corporation	Hardware Version: SAR-8, SAR-18, SAR-Ax, SAR-H, SAR-Hc, SAR-W, SAR-Wx, SAR-X; Firmware Version: SAR-OS Rel 8.0R6
3257	08/09/2018	WiLink(TM) 8 Cryptographic Engine	Texas Instruments Inc.	Hardware Version: WL1837MOD; Firmware Version: 100860185
3258	08/09/2018	Cisco Firepower Threat Defense on Cisco Firepower 2100 Series Appliances	Cisco Systems, Inc.	Hardware Version: FP2110, FP2120, FP2130 and FP2140 with FIPS Kit (AIR-AP-FIPSKIT=) and opacity shield 69-100250-01; Firmware Version: 6.2
3259	08/13/2018	Embedded Module and Embedded Module Lite	Persistent Systems, LLC	Hardware Version: P/Ns WR-5200, Version 4.0 and WR-5250, Version 1.0; Firmware Version: 19.3.2
3261	08/14/2018	Cisco Firepower Cryptographic Module	Cisco Systems, Inc.	Firmware Version: 6.2
3262	08/14/2018	TCT Crypto Engine Core	TCL Communication Ltd.	Hardware Version: 5.3.4
3263	08/16/2018	ARM® TrustZone® CryptoCell-712	ARM LIMITED	Hardware Version: 712; Firmware Version: (TEE) 1.1.0.48, (REE) 1.1.0.49 and (TEE ROM) 1.0.0.1145
3264	08/20/2018	MediaTek CryptoCore	MediaTek Inc.	Hardware Version: 1.0; Firmware Version: 1.0
3265	08/23/2018	Ultrastar® DC HC310 and Ultrastar® DC HC320 TCG Enterprise HDD	Western Digital Corporation	Hardware Version: P/Ns HUS726T4TAL4205 (1) [1, 2, 3, 5], HUS726T4TAL5205 (1) [1, 2, 3], HUS726T4TALS205 (1) [1, 2, 3], HUS726T6TAL4205 (1) [1, 2, 3, 5], HUS726T6TAL5205 (1) [1, 2, 3], HUS728T8TAL4205 (1) [4] and HUS728T8TAL5205 (1) [4]; Firmware Version: R40C [1], R40H [2], R40K [3], R410 [4] or R41C [5]
3266	08/23/2018	HID Global Cryptographic Module	HID Global Corporation	Software Version: 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
3267	08/23/2018	Cisco Adaptive Security Appliance (ASA) Virtual	Cisco Systems, Inc.	Software Version: 9.8
3268	08/24/2018	SafeNet PCIe Hardware Security Module and SafeNet PCIe Hardware Security Module for SafeNet Network HSM	Gemalto	Hardware Version: VBD-05-0100 [1, 2], VBD-05-0101 [1, 2], VBD-05-0102 [1, 2] and VBD-05-0103 [1, 2]; Firmware Version: 6.24.6 [1] and 6.24.7 [2]
3269	08/28/2018	AIX FIPS Crypto Module for OpenSSL	IBM Corporation	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
3270	08/29/2018	Red Hat Enterprise Linux NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: 6.0
3271	08/29/2018	Ultrastar® SS300 TCG Enterprise SSD	Western Digital Corporation	Hardware Version: P/Ns HUSTR7676ASS205 (1) [1, 2, 3], HUSTR7638ASS205 (1) [1, 3], HUSTR7619ASS205 (1) [1, 3], HUSTR7696ASS205 (1) [1, 3] and HUSTR7648ASS205 (1) [1, 2, 3]; Firmware Version: R500 [1], R512 [2] or R520 [3]
3272	08/29/2018	TI SimpleLink WiFi MCU HW Crypto Engines Module	Texas Instruments, Inc.	Hardware Version: Chip ID 0x311001; Firmware Version: 4.0.0.5 Chip ID 0x311001
3273	08/29/2018	CryptoComply for Server	SafeLogic Inc.	Software Version: 2.2
3274	08/30/2018	iStorage diskAshur PRO^2 Level 3 Secure Storage Drive	iStorage Ltd.	Hardware Version: IS-DAP2-256-500-C-X, IS-DAP2-256-1000-C-X, IS-DAP2-256-2000-C-X, IS-DAP2-256-3000-C-X, IS-DAP2-256-4000-C-X, IS-DAP2-256-5000-C-X, IS-DAP2-256-SSD-128-C-X, IS-DAP2-256-SSD-256-C-X, IS-DAP2-256-SSD-512-C-X, IS-DAP2-256-SSD-1000-C-X, IS-DAP2-256-SSD-2000-C-X, IS-DAP2-256-SSD-4000-C-X; Firmware Version: EC Firmware version IS_EC_FW_2_59_1X and SC Firmware version 3.1
3275	08/30/2018	Centrify Cryptographic Module	Centrify Corporation	Software Version: 2.0 [1], 2.1 [2]
3276	08/30/2018	Cisco Firepower Next-Generation IPS Virtual (NGIPSv) Cryptographic Module	Cisco Systems, Inc.	Software Version: 6.2