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 2019

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: Michael D Cooper

Dated: 9/17/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: September 11, 2019

Manager, Product Assurance and Standards
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
3501	08/01/2019	BitLocker(R) Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016	Microsoft Corporation	Software Version: 10.0.14393.1770
3502	08/01/2019	BitLocker(R) Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016	Microsoft Corporation	Software Version: 10.0.14393.1770
3503	08/01/2019	KeyPair FIPS Object Module for OpenSSL	KeyPair Consulting Inc.	Software Version: 1.0
3504	08/08/2019	AsigraEncModule Encryption Library	Asigra Inc.	Software Version: 2.0
3505	08/08/2019	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module	RSA	Software Version: 6.2 [1], 6.2.1.1 [2] and 6.2.1.2 [3]
3506	08/08/2019	PowerMax NVMe and VMAX 12G SAS Module	Dell EMC	Hardware Version: 303-493-001C-03 [1]; and 303-305-100A-06 [2]; Firmware Version: v3.09.34.00 [1]; and v3.08.41.00 [2]
3507	08/08/2019	Riverbed XD Series Wi-Fi Products	Riverbed Technology, Inc.	Hardware Version: P/Ns XD2-240-FIPS, XD4-240-FIPS, XA4-240-FIPS, XD2-230-FIPS and XH2-240-FIPS with XE-6000-TBAR (Enclosure Form Factor) and with SKU XE-LABEL-FIPS (Tamper-Evident Seals); Firmware Version: AOS-8.6
3508	08/09/2019	TMC TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type A1	Toshiba Memory Corporation	Hardware Version: A2 with PX04SVQ080B, A2 with PX04SVQ160B, A2 with PX04SRQ384B; Firmware Version: NA03
3509	08/09/2019	TMC TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type B1	Toshiba Memory Corporation	Hardware Version: A1 with PX04SVQ080B, A1 with PX04SVQ160B; Firmware Version: MS01

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3510	08/09/2019	Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016	Microsoft Corporation	Software Version: 10.0.14393.1770
3511	08/12/2019	Intel® Optane™ DC SSD D4800X	Intel Corporation	Hardware Version: P/Ns [SSDPD21K375GAR with components J26977-100 rev2 and J29722-002 rev7], [SSDPD21K750GAR with components J26979-100 rev2 and J29722-002 rev7] and [SSDPD21K015TAR with components J26980-100 rev2 and J29722-002 rev7]; K33839-001 (Tamper-Evident Seals); Firmware Version: E201EF06
3512	08/21/2019	ASTRO CDEM Motorola Advanced Crypto Engine (MACE)	Motorola Solutions, Inc.	Hardware Version: P/Ns 5185912Y01, 5185912Y03 and 5185912Y05; Firmware Version: R01.03.00
3513	08/22/2019	Secure Kernel Code Integrity (skci.dll) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016	Microsoft Corporation	Software Version: 10.0.14393.1770
3514	08/23/2019	BC-FJA (Bouncy Castle FIPS Java API)	Legion of the Bouncy Castle Inc.	Software Version: 1.0.2
3515	08/29/2019	Cisco Network Convergence System 2000 Series Cryptographic Module	Cisco Systems, Inc.	Hardware Version: NCS2002, NCS2006 and NCS2015 with FIPS Kit (AIR-AP-FIPSKITx7 and AIR-AP-FIPSKITx8) and other components identified in Security Policy section 2.1; Firmware Version: 11.0
3516	08/30/2019	FortiGate-2000E/2500E	Fortinet, Inc.	Hardware Version: C1AF49 and C1AF51 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: FortiOS 5.4, b3145, 170602