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

January 2017

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: 8 Feb 2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Tony Hill

Dated: 6 Feb 2017

Director, Architecture and Technology Assurance
Communications Security Establishment

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2811	01/05/2017	Samsung SAS 12G TCG Enterprise SSC SEDs PM1633a Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILS7T6HMLS-000H9 and MZILS15THMLS-000H9; Firmware Version: 3P00
2812	01/11/2017	SSL Visibility Appliance	Symantec Corporation	Hardware Version: SV1800-C [1], SV1800B-C [2], SV1800-F [3], SV1800B-F [4], SV2800 [5] and SV2800B [6]; 090-03061 [1], 080-03560 [1], 080-03676 [1], 090-03547 [2], 080-03779 [2], 080-03784 [2], 090-03062 [3], 080-03561 [3], 080-03677 [3], 090-03548 [4], 080-03780 [4], 080-03785 [4], 090-03063 [5], 080-03562 [5], 080-03678 [5], 090-03549 [6], 080-03781 [6], 080-03786 [6] with FIPS Kit: FIPS-LABELS-SV; Firmware Version: 3.8.2F build 227, 3.8.4FC, 3.10 build 40
2813	01/11/2017	TOPDLv2.1 Platform	Gemalto SA	Hardware Version: NXP P60D144P VA (MPH149); Firmware Version: TOPDLV2.1 (Filter04), Demonstration Applet version V1.3
2814	01/11/2017	CryptoServer Se-Series Gen2	Utimaco IS GmbH	Hardware Version: 5.01.2.0 and 5.01.4.0; Firmware Version: 5.0.10.1
2815	01/12/2017	CTERA Crypto Module	CTERA Networks Ltd.	Software Version: 2.1
2816	01/12/2017	Proteus MX Licensed Band Radio Cryptographic Module	Microwave Networks Inc.	Hardware Version: P/Ns 8209361-10 Rev A03 [1], 8209361-12 Rev A03 [1], 8209361-14 Rev A03 [1], 8209363-10 Rev A03 [2], 8209363-12 Rev A03 [2] and 8209363-14 Rev A03 [2]; Firmware Version: 8746006-02 Rev A02 [1] or 8746007-02 Rev A02 [2]
2817	01/13/2017	Hypori FIPS Object Module for OpenSSL	Hypori, Inc.	Software Version: 2.0.10
2818	01/18/2017	Cisco ASA Service Module (SM)	Cisco Systems, Inc.	Hardware Version: WS-SVC-ASA-SM1-K9; Firmware Version: 9.6
2819	01/19/2017	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX05S model) Type A	Toshiba Corporation	Hardware Version: A1 with PX05SVQ080B, A1 with PX05SVQ160B or A1 with PX05SRQ384B; Firmware Version: PX05NA00
2820	01/23/2017	Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40 and 5585-X SSP-60 Adaptive Security Appliances	Cisco Systems, Inc.	Hardware Version: ASA 5506-X[1], ASA 5506H-X[1], ASA 5506W-X[1], ASA 5508-X[2][3], ASA 5512-X[2], ASA 5515-X[5], ASA 5516-X[2][4], ASA 5525-X[5], ASA 5545-X[5], ASA 5555-X[5], ASA 5585-X SSP-10[6], 5585-X SSP-20[6], 5585-X SSP-40[6], and 5585-X SSP-60[6] with [ASA5506-FIPS-KIT=][1], [ASA5500X-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3], [ASA5516-FIPS-KIT=][4], [CISCO-FIPS-KIT=][5] or [ASA5585-X-FIPS-KIT][6]; Firmware Version: 9.6
2821	01/25/2017	SSL Visibility Appliance	Symantec Corporation	Hardware Version: SV3800 [1], SV3800B [2] and SV3800B-20 [3]; 090-03064 [1], 080-03563 [1], 080-03679 [1], 090-03550 [2], 080-03782 [2], 080-03787 [2], 090-03551 [3], 080-03783 [3], and 080-03788 [3] with FIPS Kit: FIPS-LABELS-SV; Firmware Version: 3.8.2F build 227, 3.8.4FC, 3.10 build 40

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2822	01/25/2017	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX05S model) Type B	Toshiba Corporation	Hardware Version: A1 with PX05SVQ160B or A1 with PX05SVQ320B; Firmware Version: PX05MS00
2823	01/26/2017	Kanega Watch	UnaliWear, Inc.	Software Version: 3.9.2
2824	01/30/2017	Aegis Secure Key 3Z Cryptographic Module	Apricorn, Inc.	Hardware Version: RevA [P/Ns ASK3Z-8GB (8GB), ASK3Z-16GB (16GB), ASK3Z-32GB (32GB), ASK3Z-64GB (64GB) and ASK3Z-128GB (128GB)]; Firmware Version: 7.1
2825	01/30/2017	eToken 5110	Gemalto	Hardware Version: P/Ns STM32F042K6U6TR [1] and SLE78CFX3000PH [2]; Firmware Version: 5110 FIPS FW ver-15.0 [1] and IDCore30-revB- Build 06, eToken Applet version 1.8, eTPnP Applet V1.0 [2]
2826	01/31/2017	DataLocker H350	DataLocker Inc.	Hardware Version: P/Ns MXKB1B500G5001FIPS, MXKB1B001T5001FIPS, MXKB1B002T5001FIPS, DL-H350-0250SSD, DL-H350-0500SSD, DL-H350-1000SSD; Firmware Version: 1.1.0
2931	01/26/2017	Boot Manager 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
2932	01/26/2017	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
2933	01/26/2017	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

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2934	01/26/2017	BitLocker(R) Dump Filter (dumpfve.sys) in 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
2935	01/26/2017	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
2936	01/26/2017	Kernel Mode Cryptographic Primitives Library (cng.sys) 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
2937	01/26/2017	Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.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

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2938	01/26/2017	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