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

June 2016

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, 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: 7/7/16

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature: G. Hill

Dated: JUL 05 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Digitally signed by Bacîu Victor
Date: 2022.02.07 07:54:06 EET
Reason: MoldSign Signature
Location: Moldova

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2600	06/02/2016	Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240
2601	06/02/2016	BitLocker(R) Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240
2602	06/02/2016	BitLocker(R) Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240
2603	06/02/2016	BitLocker(R) Dump Filter (dumpfve.sys) in Microsoft Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240
2604	06/02/2016	Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240
2605	06/02/2016	Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240
2606	06/02/2016	Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240

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
2607	06/02/2016	Secure Kernel Code Integrity (skci.dll) in Microsoft Windows 10 Enterprise, Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240
2650	06/02/2016	Cisco ASA Service Module (SM)	Cisco Systems, Inc.	Hardware Version: WS-SVC-ASA-SM1-K9; Firmware Version: 9.4
2651	06/03/2016	Huawei FIPS Cryptographic Library (HFCL)	Huawei Technologies Co., Ltd.	Software Version: V300R003C22SPC805
2652	06/06/2016	Vormetric Data Security Manager Module	Vormetric, Inc.	Hardware Version: 3.0; Firmware Version: 5.3.0
2653	06/06/2016	Cisco Adaptive Security Appliance (ASA) Virtual	Cisco Systems, Inc.	Software Version: 9.4
2654	06/07/2016	BCM58100B0 Series: BCM5801B0, BCM5802B0, BCM5803B0	Broadcom Ltd.	Hardware Version: P/Ns BCM5801B0, BCM5802B0 and BCM5803B0; Firmware Version: rev0
2655	06/09/2016	NPCT6XX TPM 1.2	Nuvoton Technology Corporation	Hardware Version: FB5C85D and FB5C85E IN TSSOP28 PACKAGE and FB5C85D and FB5C85E IN QFN32 PACKAGE; Firmware Version: 5.81.0.0, 5.81.1.0
2656	06/09/2016	Motorola GGM 8000 Gateway	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1841E Rev AB with FIPS Kit P/N CLN8787A Rev B and Power Supply P/N CLN1850A Rev G (AC) or P/N CLN1849A Rev H (DC); Firmware Version: KS-16.8.1.06
2657	06/13/2016	Red Hat Enterprise Linux libgcrypt Cryptographic Module v4.0	Red Hat(R), Inc.	Software Version: 4.0
2658	06/15/2016	Rubrik Cryptographic Library	Rubrik Inc.	Software Version: 1.0
2659	06/16/2016	eSRVIVR(r) Cockpit Voice and Flight Data Recorder (CVFDR) Encryption Module	L-3 Communications, Aviation Recorders	Firmware Version: 1.0
2660	06/16/2016	Samsung SAS 12G TCG Enterprise SSC SEDs PM163x Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILS3T8HCJM-000D8 [1], MZILS3T8HCJM-000G6 [2]; Firmware Version: CXP2 [1], NA00 [2]
2661	06/16/2016	HPE 6125XLG Blade Switches	Hewlett Packard(R), Enterprise	Hardware Version: HPE 6125XLG; Firmware Version: 7.1.045
2662	06/17/2016	LG Framework Cryptographic Module	LG Electronics, Inc.	Software Version: 1.0.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2663	06/20/2016	PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series and PA-7050 Firewalls	Palo Alto Networks	Hardware Version: PA-200 P/N 910-000015-00E Rev. E [1], PA-500 P/N 910-000006-00O Rev. O [2], PA-500-2GB P/N 910-000094-00O Rev. O [2], PA-2020 P/N 910-000004-00Z Rev. Z [3], PA-2050 P/N 910-000003-00Z Rev. Z [3], PA-3020 P/N 910-000017-00J Rev. J [4], PA-3050 P/N 910-000016-00J Rev. J [4], PA-4020 P/N 910-000002-00AB Rev. AB [5], PA-4050 P/N 910-000001-00AB Rev. AB [5], PA-4060 P/N 910-000005-00S Rev. S [5], PA-5020 P/N 910-000010-00F Rev. F [6], PA-5050 P/N 910-000009-00F Rev. F [6], PA-5060 P/N 910-000008-00F Rev. F [6] and PA-7050 P/N 910-000102-00B with 910-000028-00B Rev. B [7]; FIPS Kit P/Ns: 920-000084-00A Rev. A [1], 920-000005-00A Rev. A [2], 920-000004-00A Rev. A [3], 920-000081-00A Rev. A [4], 920-000003-00A Rev. A [5], 920-000037-00A Rev. A [6] and 920-000112-00A Rev. A [7]; Firmware Version: 6.0.13
2664	06/20/2016	ACOS5-64	Advanced Card Systems Ltd.	Hardware Version: ACOS5-64; Firmware Version: 3.00
2665	06/21/2016	CoSign	ARX (Algorithmic Research)	Hardware Version: 7.0 and 8.0; Firmware Version: 8.0
2666	06/29/2016	PTP 700 Point to Point Wireless Ethernet Bridge	Cambium Networks, Ltd.	Hardware Version: P/Ns C045070B001A, C045070B002A, C045070B003A, C045070B004A, C045070B005A, C045070B006A, C045070B007A, C045070B008A, C045070B009A, C045070B010A, C045070B011A, C045070B012A, C045070B013A, C045070B014A, C045070B015A, C045070B016A, C045070B017A, C045070B018A, C045070B019A, C045070B020A, C045070B021A, C045070B022A, C045070B023A, C045070B024A, C045070B025A, C045070B026A, C045070B027A, C045070B028A, C045070B029A and C045070B030A; Firmware Version: 700-01-00-FIPS
2667	06/30/2016	Micron S650DC(R) SAS TCG Enterprise SSC Self-Encrypting Drive	Micron Technology, LLC	Hardware Version: MTFDJAK400MBS-BAN16FCYYES / MTFDJAK400MBS-2AN16FCYY, MTFDJAK800MBS-BAN16FCYYES / MTFDJAK800MBS-2AN16FCYY, MTFDJAL1T6MBS-BAN16FCYYES / MTFDJAL1T6MBS-2AN16FCYY, MTFDJAL3T2MBS-BAN16FCYYES / MTFDJAL3T2MBS-2AN16FCYY; Firmware Version: MB13
2668	06/30/2016	Motorola Network Router (MNR) S6000	Motorola Solutions, Inc.	Hardware Version: Base Unit P/N CLN1780L Rev F with Encryption Module P/N CLN8261D Rev NA; Firmware Version: GS-16.8.1.06
2669	06/30/2016	INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit	Integrity Security Services/Green Hills Software	Software Version: 3.0.0