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

April 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 J. Cooper

Dated: 5/6/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 2019-05-02

Manager, Product Assurance and Standards
Canadian Centre for Cyber Security

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3424	04/01/2019	Management Center Virtual Appliance	Symantec Corporation	Software Version: 2.1
3425	04/01/2019	Management Center	Symantec Corporation	Hardware Version: 090-03341, 090-03342, 090-03343 with FIPS Security Kit (HW-KIT-FIPS-400); Firmware Version: 2.1
3426	04/01/2019	BitLocker(R) Windows Resume (winresume) in Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240.17643
3427	04/01/2019	BitLocker(R) Windows OS Loader (winload) in Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240.17643
3428	04/03/2019	OmniSwitch AOS 8.3.1.R01	Alcatel-Lucent Enterprise USA Inc.	Hardware Version: OmniSwitch 6860-24, OmniSwitch 6860-P24, OmniSwitch 6860-48, OmniSwitch 6860-P48, OmniSwitch 6860E-24, OmniSwitch 6860E-P24, OmniSwitch 6860E-48, OmniSwitch 6860E-P48, OmniSwitch 6860E-U28, OmniSwitch 6865-P16X, OmniSwitch 6900-X20, OmniSwitch 6900-X40, OmniSwitch 6900-T20, OmniSwitch 6900-T40, OmniSwitch 6900-Q32, and OmniSwitch 6900-X72; FIPS Kit P/N: OS-FIPSKIT; Firmware Version: AOS 8.3.1.R01
3429	04/04/2019	EOS MACsec Alpha Hybrid Module	Arista Networks Inc.	Hardware Version: P/Ns Chassis: DCS-7508N, Version 06.00; DCS-7512N, Version 00.06; DCS-7516N, Version 10.00; {Supervisor with Renesas Security chip (R5H30211 or N313X): DCS-7500E-SUP, Version 01.02; DCS-7500-SUP2-D, Version 03.03; DCS-7516-SUP2, Version 10.00}; {MACsec Linecard with Broadcom MACsec chip (BCM82391): DCS-7500RM-36CQ-LC, Versions 11.01, 10.02, 10.01; DCS-7500R-8CFPX-LC, Version 11.02}; Firmware Version: 1.0
3430	04/04/2019	Primus HSM	Securosys SA	Hardware Version: P/Ns E20 / 60-1004 Rev0, E60 / 60-1004 Rev0, E150 / 60-1004 Rev0, EP700 / 60-1008 Rev0, X200 / 60-1002 Rev1, X400 / 60-1002 Rev1, X700 / 60-1002 Rev1 and X1000 / 60-1010 Rev1; Firmware Version: 2.5.3
3431	04/04/2019	Apple CoreCrypto Kernel Module v9.0 for Intel	Apple Inc.	Software Version: 9.0
3432	04/11/2019	Allegro Cryptographic Engine	Allegro Software Development Corporation	Software Version: 6.3
3433	04/11/2019	Apple CoreCrypto Module v9.0 for ARM	Apple Inc.	Software Version: 9.0
3434	04/15/2019	Qualcomm(R) Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.4.2
3435	04/19/2019	VMware's IKE Crypto Module	VMware, Inc.	Software Version: 1.1.0
3436	04/19/2019	BCM58200 Series: BCM58201, BCM58202	Broadcom Ltd.	Hardware Version: P/Ns BCM58201A0KFBG and BCM58202PA0KFBG; Firmware Version: 8bc25ceb540a57ed8fdbb2104b6751c6b1d0450f of June 27, 2018

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3437	04/23/2019	Code Integrity (ci.dll) in Windows 10 Enterprise LTSB	Microsoft Corporation	Software Version: 10.0.10240.17643
3438	04/23/2019	Apple CoreCrypto Kernel Module v9.0 for ARM	Apple Inc.	Software Version: 9.0
3439	04/23/2019	F5(R) vCMP Cryptographic Module	F5 Networks	Firmware Version: 13.1.1 EHF
3441	04/26/2019	TAISYS JUISE-S2	Taisys Technologies Co., Ltd.	Hardware Version: 46 43; Firmware Version: 32 53
3442	04/26/2019	Vormetric Data Security Manager Module	Thales eSecurity	Hardware Version: 3.0; Firmware Version: 6.0.2
3443	04/26/2019	Vormetric Data Security Manager Virtual Appliance Module	Thales e-Security	Software Version: 6.0.2
3444	04/26/2019	Standalone IMB	GDC Technology Limited	Hardware Version: GDC-IMB-v4; Firmware Version: 3.2, Security Manager Firmware Version 1.7.1
3445	04/29/2019	Endpoint Security Module	Silver Spring Networks, Inc.	Hardware Version: 130-0117-01.ESM; Firmware Version: ROM version 82136 with Applet version 1.0.0
3446	04/29/2019	Christie IMB-S3 4K Integrated Media Block (IMB)	Christie Digital Systems Canada Inc.	Hardware Version: 000-105081-03; Firmware Version: 2.1.5-4575 and 2.1.5-4582
3447	04/29/2019	Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, Windows 10 for Surface Hub	Microsoft Corporation	Software Version: 10.0.10586.1176
3448	04/30/2019	Honeywell Mobility Edge™ BoringCrypto	Honeywell International, Inc	Software Version: 1.0