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

Consolidated Certificate No. 0051

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 J Cooper

Dated: 4/1/15

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: Apr. 1st 2015

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2330	03/03/2015	Protegrity Cryptographic Module	Protegrity USA Inc.	Software Version: 1.0
2331	03/03/2015	Aspen	Sony Corporation	Hardware Versions: 1.0.0 and 1.1.0; Firmware Version: 1.3.0
2332	03/03/2015	XTM 850 [1], XTM 860 [2], XTM 870 [3], XTM 870-F [4], XTM 1520 [5], XTM 1520-RP [6], XTM 1525 [7], XTM 1525-RP [8], XTM 2520 [9]	WatchGuard Technologies, Inc.	Hardware Versions: SL8AE14 [1-5,7], SL15AE14 [6,8], SL25AE14F4 [9] with Tamper Evident Seal Kit: SKU WG8566; Firmware Version: Fireware XTM OS v11.6.5
2333	03/03/2015	Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive	Toshiba Corporation	Hardware Version: A0 with AL13SXQ300NB, AL13SXQ450NB or AL13SXQ600NB; Firmware Version: 0101
2334	03/05/2015	Dell W-IAP155 and W-IAP155P Wireless Access Points with Dell AOS FIPS Firmware	Dell, Inc.	Hardware Versions: W-IAP155-F1, W-IAP155-USF1, W-IAP155P-F1 and W-IAP155P-USF1 with Aruba FIPS kit 4010061-01; Firmware Version: ArubaOS 6.3.1.7-FIPS
2335	03/11/2015	Dell W-AP92, W-AP93, W-AP104, W-AP105, and W-AP175 Wireless Access Points with Dell AOS FIPS Firmware	Dell, Inc.	Hardware Versions: W-AP92-F1, W-AP93-F1, W-AP104-F1, W-AP105-F1, W-AP175P-F1, W-AP175AC-F1 with Aruba FIPS kit 4010061-01; Firmware Version: ArubaOS 6.3.1.7-FIPS
2336	03/11/2015	3e-636M-HSE CyberFence Cryptographic Module	3e Technologies International, Inc.	Hardware Version: 1.0; Firmware Version: 5.0
2337	03/16/2015	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: SKC1.5
2338	03/16/2015	HiCOS Combi PKI Native Smart Card	Chunghwa Telecom Co., Ltd.	Hardware Versions: RS46X and RS47X; Firmware Version: HardMask: 2.3 and SoftMask: 3.5
2339	03/20/2015	Dell W-AP224 and W-AP225 Wireless Access Points with Dell AOS FIPS Firmware	Dell, Inc.	Hardware Versions: W-AP224-F1 and W-AP225-F1 with Aruba FIPS kit 4010061-01; Firmware Version: ArubaOS 6.3.1.7-FIPS

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
2340	03/20/2015	Symantec NetBackup Cryptographic Module	Symantec Corporation	Software Version: 1.0
2341	03/20/2015	Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches	Cisco Systems, Inc.	Hardware Versions: Cisco Catalyst 3650 Series Switches, Cisco Catalyst 3850 Series Switches [1] and Cisco Field Replaceable Uplink Network Modules [1]; Firmware Version: IOS XE 03.06.00aE
2342	03/24/2015	Vormetric Encryption Expert Cryptographic Module	Vormetric, Inc.	Hardware Version: E5-2670; Software Version: 5.1.3
2343	03/24/2015	Vormetric Encryption Expert Cryptographic Module	Vormetric, Inc.	Software Version: 5.1.3
2351	03/12/2015	Boot Manager in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series	Microsoft Corporation	Software Versions: 6.3.9600 and 6.3.9600.17031