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

October 2015

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: 11/23/2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature:

Dated: NOV 10 2015

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2455	10/14/2015	SHIELD Secure Coprocessor	SiCore Technologies Inc.	Hardware Version: SHIELD Secure CoProcessor V1.0; Firmware Version: MFF V1.0, FPGA V1.0, SC V1.0
2456	10/21/2015	Acme Packet 3820 and Acme Packet 4500	Oracle Corporation	Hardware Version: A1; Firmware Version: ECx6.4.1 and ECx6.4.1M1
2457	10/22/2015	Aruba 7XXX Series Controllers with ArubaOS FIPS Firmware	Aruba Networks, Inc.	Hardware Version: Aruba 7005-F1, Aruba 7005-USF1, Aruba 7010-F1, Aruba 7010-USF1, Aruba 7024-F1, Aruba 7024-USF1, Aruba 7030-F1, Aruba 7030-USF1, Aruba 7205-F1 and Aruba 7205-USF1 with FIPS kit 4011570-01; Firmware Version: ArubaOS 6.4.3-FIPS
2458	10/22/2015	Barracuda Cryptographic Software Module	Barracuda Networks	Software Version: 1.0.1.8
2460	10/27/2015	Astro Subscriber Motorola Advanced Crypto Engine (MACE) - Security Level 2	Motorola Solutions, Inc.	Hardware Version: P/Ns 5185912Y01, 5185912Y03, 5185912Y05 and 5185912T05; Firmware Version: R01.07.25 and [R01.00.00 or (R01.00.00 and R02.00.00)]
2461	10/27/2015	Astro Subscriber Motorola Advanced Crypto Engine (MACE) - Security Level 3	Motorola Solutions, Inc.	Hardware Version: P/Ns 5185912Y01, 5185912Y03, 5185912Y05 and 5185912T05; Firmware Version: R01.07.25 and [R01.00.00 or (R01.00.00 and R02.00.00)]
2462	10/29/2015	Hitachi Virtual Storage Platform (VSP) Encryption Module	Hitachi, Ltd.	Hardware Version: P/N: 3289094-A(BS12GE) Version: B/D4 or B/D5; Firmware Version: 03.07.49.00
2463	10/30/2015	Accellion Cryptographic Module	Accellion, Inc.	Software Version: FTALIB_4_0_1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2464	10/30/2015	SUSE Linux Enterprise Server 12 libgcrypt Cryptographic Module	SUSE, LLC	Software Version: 1.0
2465	10/30/2015	Mobile Application Cryptographic Module	Silent Circle	Software Version: 1.0
2466	10/30/2015	Enhanced Bandwidth Efficient Modem (EBEM) Cryptographic Module	ViaSat, Inc.	Hardware Version: P/Ns 1010162 Version 1, 1010162 with ESEM Version 1, 1091549 Version 1, 1075559 Version 1, 1075559 with ESEM Version 1, 1091551 Version 1, 1010163 Version 1, 1010163 with ESEM Version 1, 1091550 Version 1, 1075560 Version 1, 1075560 with ESEM Version 1, 1091552 Version 1, and 1047117; Firmware Version: 02.06.17
2467	10/30/2015	Purity Encryption Module	Pure Storage, Inc.	Software Version: 1.1.0; Hardware Version: Intel Xeon x64 CPU E5-2670 v2
2468	10/30/2015	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module	RSA, the Security Division of EMC	Software Version: 6.2
2469	10/30/2015	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module	RSA, the Security Division of EMC	Software Version: 6.2