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

April 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 A Cooper

Dated: 5/2/2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature:

Dated: 2 May 2016

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2598	04/01/2016	HPE Enterprise Secure Key Manager	Hewlett Packard Enterprise	Hardware Version: P/Ns C8Z61AA, Versions 4.0 [1] and 4.1 [2]; Firmware Version: 6.0.0-51 [1] and 6.1.0-14 [2]
2599	04/01/2016	Cleversafe FIPS Cryptographic Module	Cleversafe, Inc.	Software Version: 1.1
2608	04/05/2016	SBC 5110 and 5210 Session Border Controllers	Sonus Networks, Inc.	Hardware Version: SBC 5110 and SBC 5210; Firmware Version: 5.0
2609	04/05/2016	Apple iOS CoreCrypto Kernel Module v6.0	Apple Inc.	Software Version: 6.0
2610	04/05/2016	Apple OS X CoreCrypto Module, v6.0	Apple Inc.	Software Version: 6.0
2611	04/07/2016	Java Crypto Module	Silent Circle	Software Version: 1.0
2612	04/08/2016	QTI Pseudo Random Number Generator	Qualcomm Technologies, Inc.	Hardware Version: 2.0
2613	04/11/2016	SR-OS Cryptographic Module	Nokia Corporation	Firmware Version: 13.0R4
2614	04/11/2016	QTI Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.3.1
2615	04/12/2016	AirTight Wireless Sensor	AirTight Networks, Inc.	Hardware Version: C-75 and C-75-E with Tamper Evident Seal Kit: C-TPL-A; Firmware Version: 7.2.FIPS.04
2616	04/18/2016	PA-3060 and PA-7080 Firewalls	Palo Alto Networks	Hardware Version: PA-3060 P/N 910-000104-00C Rev. C and PA-7080 P/N 910-000122-00A with 910-000028-00B or 910-000117-00A; FIPS Kit P/Ns: 920-000138-00A Rev. A and 920-000119-00A Rev. A; Firmware Version: 7.0.1-h4 and 7.0.3
2617	04/18/2016	WildFire WF-500	Palo Alto Networks	Hardware Version: P/N: 910-000097-00G Rev G; FIPS Kit P/N: 920-000145 Version Rev 00A; Firmware Version: 7.0.3
2618	04/19/2016	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: 9.4
2619	04/19/2016	Vocera Cryptographic Module v3.0	Vocera Communications, Inc.	Software Version: 3.0; Hardware Version: 88W8787; Firmware Version: 3.0
2620	04/21/2016	Palo Alto Networks VM-Series	Palo Alto Networks	Software Version: 7.0.1-h4 or 7.0.3
2621	04/21/2016	Websense C Cryptographic Module	Forcepoint	Software Version: 2.1

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
2622	04/22/2016	SUSE Linux Enterprise Server 12 - NSS Module	SUSE, LLC	Software Version: 1.0
2623	04/25/2016	Veritas Cryptographic Module	Veritas Technologies LLC	Software Version: 1.0
2624	04/27/2016	Teamcenter Cryptographic Module	Siemens PLM Software Inc.	Software Version: 3.0
2625	04/28/2016	ECI TR10_4EN Encryption Module	ECI Telecom Ltd.	Hardware Version: Board-Type=0x856B, Revision# D3; Firmware Version: R6.3
2626	04/14/2016	mToken CryptoID	Century Longmai Technology Co. Ltd	Hardware Version: SCC-X; Firmware Version: 3.11
2627	04/28/2016	NPCT6XX TPM 2.0	Nuvoton Technology Corporation	Hardware Version: FB5C85D and FB5C85E IN TSSOP28 PACKAGE and FB5C85D and FB5C85E IN QFN32 PACKAGE; Firmware Version: 1.3.0.1
2628	04/28/2016	StarSign Crypto-USB Token S powered by Sm@rtCafé Expert 7.0 Secure Element	Giesecke & Devrient GmbH	Hardware Version: SLE78CUFX5000PH (M7893 B11); Firmware Version: Sm@rtCafé Expert 7.0, Demonstration Applet V1.0