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. 0056

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: 9/2/2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: D.J. McPhee

Dated: 2 September 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
2403	8/11/2015	Luna® G5 Cryptographic Module	SafeNet, Inc.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.4
2419	08/05/2015	HP TippingPoint Intrusion Prevention System	Hewlett-Packard TippingPoint	Hardware Versions: 2600NX, 5200NX, 6200NX, 7100NX, and 7500NX with HP FIPS Security Enclosure: Part# JC856A; Firmware Version: 3.8.0
2420	08/05/2015	IBM® Crypto for C	IBM® Corporation	Software Version: 8.4.1.0
2421	08/06/2015	Cisco Aironet 1142, 1262, 1532e/i, 1552e/i, 1572, 1602e/i, 1702, 2602e/i, 2702e/i, 3502e/i, 3602e/i/p and 3702e/i/p Wireless LAN Access Points	Cisco Systems, Inc.	Hardware Versions: {1142[2], 1262[3], 1532e[6], 1532i[6], 1552e[3], 1552i[3], 1572[5], 1602e[4], 1602i[4], 1702[5], 2602e[5], 2602i[5], 2702e[5], 2702i[5], 3502e[3], 3502i[3], 3602e[1,5], 3602i[1,5], 3602p[1,5], 3702e[1,5], 3702i[1,5] and 3702p[1,5] with AIR-RM3000M[1], Marvell 88W8363P[2], Marvell 88W8364[3], Marvell 88W8763C[4], Marvell 88W8764C[5] and Qualcomm Atheros AES-128w10i[6]} with FIPS Kit: AIRLAP-FIPSKIT=, VERSION B0; Firmware Version: 8.0 with IC2M v2.0
2422	8/11/2015	Nimble Storage OpenSSL FIPS Object Module	Nimble Storage Inc.	Software Version: 2.0.9
2423	8/11/2015	QTI Cryptographic Module on Crypto 5 Core	Qualcomm Technologies, Inc.	Hardware Version: Snapdragon 810; Software Version: 5.f2-64
2424	8/11/2015	DVP-200	Rockwell Collins	Hardware Versions: 822-2506-002 (Rev B or Rev C), 822-2506-003 (Rev B or Rev C) and 822-2506-004 (Rev C or Rev D); Firmware Versions: 811-4562-004 and 811-4563-002
2425	8/11/2015	wolfCrypt	wolfSSL Inc.	Software Version: 3.6.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2426	8/11/2015	Luna® G5 Cryptographic Module	SafeNet, Inc.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.4
2427	8/11/2015	Luna® PCI-E Cryptographic Module	SafeNet, Inc.	Hardware Versions: VBD-05, Version Code 0100, VBD-05, Version Code 0101, VBD-05, Version Code 0103; Firmware Version: 6.10.4
2428	8/11/2015	Luna® PCI-E Cryptographic Module	SafeNet, Inc.	Hardware Versions: VBD-05, Version Code 0100, VBD-05, Version Code 0101, VBD-05, Version Code 0103; Firmware Version: 6.10.4
2429	8/11/2015	Luna® Backup HSM Cryptographic Module	SafeNet, Inc.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.4
2430	8/14/2015	Samsung Kernel Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: SKC1.6
2431	08/19/2015	iStorage datAshur SSD 3.0 Cryptographic Module	iStorage Limited	Hardware Version: RevD; Firmware Version: 6.5
2432	08/19/2015	DIGIPASS GO-7	VASCO Data Security International, Inc.	Hardware Version: DIGIPASS GO-7 FIPS 140-2; Firmware Version: 0355
2433	08/19/2015	Websense Java Crypto Module	Websense, Inc.	Software Version: 2.0.1
2434	08/20/2015	ProtectServer Internal Express 2 (PSI-E2)	SafeNet, Inc.	Hardware Version: VBD-05, Version Code 0200; Firmware Version: 5.00.02
2435	08/20/2015	SUSE Linux Enterprise Server 12 - OpenSSL Module	SUSE, LLC	Software Version: 2.0
2436	08/26/2015	EDK Management Module	Huawei Device (Dongguan) Co. Ltd.	Software Version: P7-L00V100R001C17B210

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2437	08/26/2015	HID Global ActivID Applet Suite v2.6.2B on Oberthur Technologies ID-One Cosmo V7	HID Global	Hardware Versions: P/Ns B0, BA, C4 and C7; Firmware Version: FC10 / 069778 with HID Global ActivID Applet Suite Version 2.6.2B.7