FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0054

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: 7/13/15

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 13 July 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
2378	06/19/2015	ChaseSun CS100	ChaseSun Information Security Technology Development (Beijing) Co., Ltd.	Hardware Version: 1.0.0; Firmware Version: 1.0.0
2389	06/02/2015	SafeZone FIPS Cryptographic Module	INSIDE Secure	Software Version: 1.1.0
2390	06/19/2015	SPYCOS® 3.0 QFN	SPYRUS, Inc.	Hardware Version: 742100003F; Firmware Version: 3.0
2391	06/11/2015	HP TippingPoint Crypto Core OpenSSL	Hewlett-Packard TippingPoint	Software Version: 2.0.8
2392	06/15/2015	ID-One PIV on Cosmo V8	Oberthur Technologies	Hardware Version: '0F'; Firmware Version: '5601'; Firmware Extension: '082371' with ID-One PIV Applet Suite 2.3.5
2393	06/15/2015	Cisco Integrated Services Router (ISR) 4451-X (with SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P, PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) and Integrated Services Router (ISR) 4431 (with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256)	Cisco Systems, Inc.	Hardware Versions: ISR 4451-X [1] and ISR 4431 [2] with SM-ES3X-16-P [1], SM-ES3X-24-P [1], SM-D-ES3X-48-P [1], PVDM4-32 [1,2], PVDM4-64 [1,2], PVDM4-128 [1,2] and PVDM4-256 [1,2]; Firmware Version: IOS-XE 3.13
2394	06/15/2015	HP TippingPoint Crypto Core NSS	Hewlett-Packard TippingPoint	Software Version: 3.12.9.1
2395	06/23/2015	ProFLEX01-R2	Syn-Tech Systems, Inc.	Hardware Versions: 450-0139 and 450-0140; Firmware Version: 4.20
2396	06/23/2015	Apple iOS CoreCrypto Module v5.0	Apple Inc.	Software Version: 5.0
2397	06/23/2015	WatchKey ProX USB Token Cryptographic Module	WatchData Technologies Pte Ltd	Hardware Version: Smart Card Chip AS518 and K023314A; Firmware Version: 36410101
2398	06/24/2015	OpenSSL FIPS Object Module SE	OpenSSL Software Foundation	Software Version: 2.0.9

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2399	06/29/2015	Dell SonicWALL NSA Series 2600, 3600, 4600, 5600	Dell Software, Inc.	Hardware Versions: P/Ns 101-500362-63, Rev. A (NSA 2600), 101-500338-64, Rev. A (NSA 3600), 101-500365-64, Rev. A (NSA 4600), 101-500360-65, Rev. A (NSA 5600); Firmware Version: SonicOS v6.2.0
2400	06/29/2015	Dell SonicWALL NSA Series SM 9600, SM 9400, SM 9200, NSA 6600	Dell Software, Inc.	Hardware Versions: P/Ns 101-500380-71, Rev. A (SM 9600), 101-500361-70, Rev. A (SM 9400), 101-500363-70, Rev. A (SM 9200), 101-500364-66, Rev. A (NSA 6600); Firmware Version: SonicOS v6.2.0
2401	06/30/2015	Kanguru Defender 3000	Kanguru Solutions	Hardware Versions: P/Ns KDF3000-4G, KDF3000-8G, KDF3000-16G, KDF3000-32G, KDF3000-64G, KDF3000-128G, Version 1.0; Firmware Version: 2.10.10