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. 0030

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: _____

Dated: 8-5-13

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 22 July 2013

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1955	06/03/2013	Kony Solutions Cryptographic Library	Kony Solutions, Inc.	Software Version: 2.0
1956	06/07/2013	Apple OS X CoreCrypto Kernel Module, v3.0	Apple Inc.	Software Version: 3.0
1957	06/11/2013	Luna® G5 Cryptographic Module	SafeNet, Inc.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.2.3
1958	06/11/2013	Luna® G5 Cryptographic Module	SafeNet, Inc.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.2.3
1959	06/12/2013	Check Point CryptoCore	Check Point Software Technologies Ltd	Software Version: 2.0
1960	06/12/2013	McAfee Firewall Enterprise Virtual Appliance for VMware ESXi 4.1	McAfee, Inc.	Software Version: 8.2.1
1961	06/14/2013	TruLink Control Logic Module CL6792-M1	Telephonics Sweden AB	Hardware Version: P/N 010.6792-01 Rev. H3; Firmware Version: Boot: SW7098 v2.5 and Application: SW7099 v9.9.1
1962	06/14/2013	Tahir Pak Crypto Library	ACES	Software Version: 2.1.1
1963	06/14/2013	Apple iOS CoreCrypto Module, v3.0	Apple Inc.	Hardware Version: A4 and A5; Software Version: 3.0
1964	06/14/2013	Apple OS X CoreCrypto Module, v3.0	Apple Inc.	Software Version: 3.0
1965	06/14/2013	Apricorn FIPS Module 140-2	Apricorn Inc.	Hardware Version: REV. A; Firmware Version: 4.0
1966	06/21/2013	IDCore 30	Gemalto	Hardware Version: SLE78CFX3009P; Firmware Version: IDCore 30 Build 1.17, Demonstration Applet version V1.0
1967	06/26/2013	TruLink Control Logic Module CL6882-M1	Telephonics Sweden AB	Hardware Version: P/N 010.6882-01 Rev. B2; Firmware Version: Boot: SW7158 v2.4 and Application: SW7151 v2.8.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1968	06/26/2013	Postal mRevenector CA 2012	Francotyp-Postalia GmbH	Hardware Version: 580036020300/01; Firmware Versions: 90.0036.0201.00/2011485001 (Bootloader), 90.0036.0206.00/2011485001 (Software-Loader) and 90.0036.0211.00/2013032001 (CA Application)
1969	06/26/2013	Authentication Token	Thales e-Security Ltd.	Hardware Version: Inside Secure AT90SC28872RCU Revision G; Firmware Version: Athena IDProtect 010B.0333.0004 with Authentication Token Applet 1.0