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

November 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 A Cooper

Dated: 14 Dec 2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature: D.C.M.

Dated: 03 December 2015

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

DAN McCARTHY, A/DIR. ATA

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2470	11/05/2015	FT-JCOS (Feitian Java Card Platform)	Feitian Technologies Co., Ltd.	Hardware Version: P/Ns SLE78CLFX4000PM [1], SLE77CLFX2400PM [2] and SLE78CLUFX5000PHM [3]; Firmware Version: 1.0.0 [1], 1.0.1 [2] and 1.0.2 [3]
2471	11/13/2015	SUSE Linux Enterprise Server 12 - OpenSSH Server Module	SUSE, LLC	Software Version: 1.0
2472	11/13/2015	SUSE Linux Enterprise Server 12 - OpenSSH Client Module	SUSE, LLC	Software Version: 1.0
2473	11/13/2015	OpenSSL FIPS Object Module RE	OpenSSL Software Foundation	Software Version: 2.0.9 or 2.0.10
2474	11/16/2015	Samsung CryptoCore Module	Samsung Electronics Co., Ltd.	Software Version: 0.2.9
2475	11/16/2015	C-ACE	Red Cocoa II L.L.C.	Hardware Version: STM32F405OG; Firmware Version: Bootloader: 0.0.1; Application: 1.0.0
2476	11/20/2015	KONA N41M0	KONA I Co., Ltd.	Hardware Version: Infineon SLE97CNFX1M00PEA22; Firmware Version: KONA N41M0 v2.01 and Demonstration Applet v1.2.4
2477	11/23/2015	IMS-SM	Dolby Laboratories, Inc.	Hardware Version: IMS-SM-C1 [A], IMS-SM-C2 [A], IMS-SM-E1 [A], IMS-SM-E2 [A], IMS2-SM-C1 [A], IMS2-SM-C2 [A] and IMS2-SM-C3 [A]; Firmware Version: (4.4.1-0, 4.2.0-3 and 6.0.12d-0) [A]
2478	11/25/2015	KONA N41M0	KONA I Co., Ltd.	Hardware Version: Infineon SLE97CNFX1M00PEA22; Firmware Version: KONA N41M0 v2.01 and PKI Applet v1.3.3