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. 0055

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 D Cooper

Dated: 18 Aug 2015

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: AUG 18 2015

Greg Wilds

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2402	07/01/2015	BlackBerry Cryptographic Tool Kit	BlackBerry Limited	Software Versions: 6.0 and 6.0.2
2404	07/06/2015	Secure Mobile	Digital Defence Ltd	Software Version: 11.1.0.0
2406	07/09/2015	AQ42-M	Digicine Oristar Technology Development (Beijing) Co., Ltd.	Hardware Version: 2.0.0; Firmware Version: 1.3.0
2407	07/22/2015	Apple iOS CoreCrypto Kernel Module v5.0	Apple Inc.	Software Version: 5.0
2408	07/22/2015	Apple OS X CoreCrypto Module, v5.0	Apple Inc.	Software Version: 5.0
2409	07/22/2015	Cisco ASR 1001, 1001-X, 1002, 1002-X, 1004, 1006 and 1013	Cisco Systems, Inc.	Hardware Versions: ASR1001, ASR1001-X, ASR1002, ASR1002-X, ASR1004, ASR1006 and ASR1013; Embedded Services Processors: ASR1000-ESP5, ASR1000-ESP10, ASR1000-ESP20, ASR1000-ESP40, ASR1000-ESP100 and ASR1000-ESP200; Route Processors: ASR-1000-RP1 and ASR-1000-RP2; Linecards: ASR1000-6TGE and ASR1000-2T+20X1GE; Firmware Version: IOS XE 3.13
2410	07/22/2015	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model NA02)	Toshiba Corporation	Hardware Version: A0 with PX02SMU020, PX02SMU040, PX02SMU080 or PX02SMQ160; Firmware Version: NA02
2411	07/22/2015	Apple OS X CoreCrypto Kernel Module v5.0	Apple Inc.	Software Version: 5.0
2412	07/22/2015	CellTrust Cryptographic Module (CTCM)	CellTrust®-Corporation	Software Version: 2.0
2413	07/23/2015	HP TippingPoint Intrusion Prevention System	Hewlett-Packard TippingPoint	Hardware Versions: S660N, S1400N, S2500N, and S5100N; Firmware Version: 3.8.0

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
2414	07/23/2015	Astro Subscriber Motorola Advanced Crypto Engine (MACE)	Motorola Solutions, Inc.	Hardware Versions: P/Ns 5185912Y01, 5185912Y03 and 5185912Y05; Firmware Versions: R01.05.12 and [R01.00.00 or (R01.00.00 and R02.00.00)]
2415	07/28/2015	IDeal Citiz™ v2.0 Open	Morpho	Hardware Versions: SLE78CFX3000P, SLE78CLFX3000P, SLE78CLFX3000PM, SLE78CFX4000P, SLE78CLFX4000P, SLE78CLFX4000PM; Firmware Version: 2.0
2416	07/30/2015	McAfee Firewall Enterprise Control Center Virtual Appliance	McAfee, Inc.	Software Version: 5.3.2 Patch 6
2417	07/30/2015	McAfee Firewall Enterprise Control Center	McAfee, Inc.	Hardware Versions: FWE-C1015 with FIPS Kit: FWE-CC-FIPS-KIT1, FWE-C2050 with FIPS Kit: FWE-CC-FIPS-KIT2, FWE-C3000 with FIPS Kit: FWE-CC-FIPS-KIT2; Firmware Version: 5.3.2 Patch 6
2418	07/30/2015	HP TippingPoint Intrusion Prevention System	Hewlett-Packard TippingPoint	Hardware Version: S6100N; Firmware Version: 3.8.0