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

May 2018

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, 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: 6/1/2018

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: June 4, 2018

Director, Security Architecture and Risk Management
Communications Security Establishment

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3181	05/02/2018	Motorola Solutions Cryptographic DLL Software Module	Motorola Solutions, Inc.	Software Version: R01.03.00
3182	05/02/2018	SafeNet Luna K7+ Cryptographic Module	Gemalto	Hardware Version: 808-000069-001, 808-000070-001; Firmware Version: 7.0.1, 7.0.2, 7.0.3
3183	05/04/2018	MPU5	Persistent Systems, LLC	Hardware Version: P/N WR-5100, Versions: 4.0.B, 4.1.B, 4.2.B, 4.2.C, 4.3.B, 4.3.C, 4.3.D, 4.4.B, 4.4.C, 4.4.D; Tamper Evident Paint P/N PROD-007; Firmware Version: 19.3.1
3184	05/22/2018	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module 6.2.4	RSA Security LLC	Software Version: 6.2.4
3185	05/23/2018	VMware BC-FJA (Bouncy Castle FIPS Java API)	VMware, Inc.	Software Version: 1.0.0
3186	05/24/2018	SAFE-Key Device	BiObex, LLC	Hardware Version: 1.4; Firmware Version: Boot 1.2.0.0, PEM 1.2.0.0, BIOS 1.2.0.0
3187	05/31/2018	NPCT7xx TPM 2.0	Nuvoton Technology Corporation	Hardware Version: LAG019 in TSSOP28 Package, LAG019 in QFN32 Package, and LAG019 in UQFN16 Package; Firmware Version: 7.2.0.1
3188	05/31/2018	Zscaler Java Crypto Module	Zscaler Inc.	Software Version: 2.1
3189	05/31/2018	REDCOM Encryption 140-2	REDCOM Laboratories, Inc.	Software Version: 3.0.1