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

March 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: 4/9/2018
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature:
Dated: 9/4/2018
Director, Security Architecture and Risk Mgmt
Communications Security Establishment

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
3089	03/22/2018	Boot Manager	Microsoft Corporation	Software Version: 10.0.15063
3090	03/22/2018	Windows OS Loader	Microsoft Corporation	Software Version: 10.0.15063
3091	03/22/2018	Windows Resume	Microsoft Corporation	Software Version: 10.0.15063
3092	03/22/2018	BitLocker Dump Filter	Microsoft Corporation	Software Version: 10.0.15063
3093	03/22/2018	Code Integrity	Microsoft Corporation	Software Version: 10.0.15063
3094	03/22/2018	Kernel Mode Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.15063
3095	03/22/2018	Cryptographic Primitives Library	Microsoft Corporation	Software Version: 10.0.15063
3143	03/01/2018	Oracle Linux 7 NSS Cryptographic Module	Oracle Corporation	Software Version: R7-2.0.0
3144	03/05/2018	Palo Alto Networks VM-Series	Palo Alto Networks	Software Version: 8.0.3
3145	03/05/2018	Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: 5.0
3146	03/07/2018	Aruba 2930F Switch Series	Hewlett Packard Enterprise	Hardware Version: JL253A, JL254A, JL258A, JL263A, JL264A; Firmware Version: WC.16.04.0011
3147	03/09/2018	Apple CoreCrypto Kernel Module v8.0 for ARM	Apple Inc.	Software Version: 8.0
3148	03/09/2018	Apple CoreCrypto Module v8.0 for ARM	Apple Inc.	Software Version: 8.0
3149	03/12/2018	Network Security Platform Sensor NS-3100, NS-3200, NS-5100 and NS-5200	McAfee LLC	Hardware Version: P/Ns IPS-NS3100 Version 1.00, IPS-NS3200 Version 1.00, IPS-NS5100 Version 1.00 and IPS-NS5200 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 8.1.17.32
3150	03/13/2018	Network Security Platform Sensor NS9100 and NS9200	McAfee, LLC	Hardware Version: P/Ns IPS-NS9100 Version 1.00 and IPS-NS9200 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.2
3151	03/14/2018	BlackRidge Technology Cryptographic Module	BlackRidge Technology International, Inc.	Software Version: 2.1
3152	03/15/2018	BC-FJA (Bouncy Castle FIPS Java API)	Legion of the Bouncy Castle Inc.	Software Version: 1.0.1
3153	03/15/2018	Network Security Platform Sensor NS7100, NS7200 and NS7300	McAfee, LLC	Hardware Version: P/Ns IPS-NS7100 Version 1.00, IPS-NS7200 Version 1.00 and IPS-NS7300 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.2
3154	03/19/2018	Zscaler Mobile Cryptographic Module	Zscaler Inc.	Software Version: 2.1
3155	03/22/2018	Apple CoreCrypto Module v8.0 for Intel	Apple Inc.	Software Version: 8.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3156	03/22/2018	Apple CoreCrypto Kernel Module v8.0 for Intel	Apple Inc.	Software Version: 8.0
3157	03/22/2018	Lenovo OpenSSL Library for ThinkSystem	Lenovo Group Limited	Software Version: 1.0
3158	03/25/2018	Gallagher OpenSSL Cryptographic Module	Gallagher Group	Software Version: 2.0.12
3159	03/26/2018	Zscaler Crypto Module	Zscaler Inc.	Software Version: 2.1
3160	03/28/2018	Neopost Postal Security Device (PSD)	Neopost Technologies, S.A.	Hardware Version: A0014227-B and A0014227-C; Firmware Version: a30.06; P/N: A0099591-A
3161	03/29/2018	Network Security Platform Sensor NS3100, NS3200, NS5100 and NS5200	McAfee, LLC	Hardware Version: P/Ns IPS-NS3100 Version 1.00, IPS-NS3200 Version 1.00, IPS-NS5100 Version 1.00 and IPS-NS5200 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.2