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

June 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 D Cooper

Dated: 7/5/2018

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 7/6/2018

Director, Security Architecture and Risk Management
Communications Security Establishment

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Digitally signed by BACIU VICTOR
Date: 2023.12.30 17:37:09 EET
Reason: MoldSign Signature
Location: Moldova

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3190	06/04/2018	SDS Cryptographic Module	Software Diversified Services	Software Version: 1.0.0
3191	06/06/2018	Mocana Cryptographic Loadable Kernel Module	Mocana Corporation	Software Version: 6.5.1f
3192	06/08/2018	FortiOS 5.4	Fortinet, Inc.	Firmware Version: 5.4, b9791, 170802
3193	06/12/2018	FortiGate-100E[1], FortiGate-201E[2], FortiGate-300D[3], FortiGate-600D[4], FortiGate-800D[5]	Fortinet, Inc.	Hardware Version: C1AE25 [1], C1AE64 [2], C1AB49 [3], C1AE11 [4] and C1AC58 [5] with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 5.4, b3141, 170602 [1], FortiOS 5.4, b3144, 170602 [2], FortiOS 5.4, b9791, 170802 [3,4,5]
3198	06/14/2018	MultiApp V4.0 Platform	Gemalto	Hardware Version: SLE78CLFX400VPH, SLE78CLFX300VPH, SLE78CLFX4000PH, SLE78CLFX3000PH, SLE78CFX4000PH, SLE78CFX3000PH; Firmware Version: MultiApp V4.0, Demonstration Applet version V9.1
3199	06/14/2018	FortiGate-3700D/3815D	Fortinet, Inc.	Hardware Version: C1AA92 and C1AE66 with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 5.4, b9791, 170802
3200	06/15/2018	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.2
3201	06/15/2018	(R)Sypher AES-256-bit FPGA Encryption Module	Analog Devices, Inc.	Hardware Version: 1.00
3202	06/19/2018	ePass2003 Token and ePass2003Auto Token	Feitian Technologies Co., Ltd.	Hardware Version: V2.0; Firmware Version: 4.0.01
3203	06/20/2018	Trusted Platform Module 2.0 SLB 9670	Infineon Technologies AG	Hardware Version: SLB 9670 (Package PG-UQFN-32-1 or PG-VQFN-32-13); Firmware Version: 7.83
3204	06/21/2018	YubiKey 4 Cryptographic Module	Yubico, Inc.	Hardware Version: SLE78CLUFX3000PH; Firmware Version: 4.4.2
3205	06/25/2018	SafeNet Luna K7 Cryptographic Module	Gemalto	Hardware Version: 808-000048-002 and 808-000066-001; Firmware Version: 7.0.1, 7.0.2, 7.0.3
3206	06/25/2018	HPE Gen9 Smart Array P-Class RAID Controllers and HPE Gen9 Smart HBA H-Class Adapter	Hewlett Packard Enterprise Development LP	Hardware Version: P240nr, P440, P440ar, P542D, P840, H240nr; Firmware Version: 6.06
3207	06/25/2018	SBC Software Edition Session Border Controller	Sonus Networks, Inc.	Software Version: R5.1.2
3208	06/26/2018	SafeNet PCIe Hardware Security Module and SafeNet PCIe Hardware Security Module for SafeNet Network HSM	Gemalto	Hardware Version: VBD-05-0100 [1, 2], VBD-05-0101 [1, 2], VBD-05-0102 [1, 2] and VBD-05-0103 [1, 2]; Firmware Version: 6.24.6 [1] and 6.24.7 [2]
3209	06/27/2018	SafeNet Backup Hardware Security Module	Gemalto	Hardware Version: LTK-03, Version Code 0102 [1, 2] and LTK-03, Version Code 0103 [1, 2]; Firmware Version: 6.24.6 [1] and 6.24.7 [2]

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3210	06/27/2018	SafeNet USB Hardware Security Module	Gemalto	Hardware Version: LTK-03, Version Code 0102 [1, 2] and LTK-03, Version Code 0103 [1, 2]; Firmware Version: 6.24.6 [1] and 6.24.7 [2]
3211	06/27/2018	SafeNet USB Hardware Security Module	Gemalto	Hardware Version: LTK-03, Version Code 0102 [1, 2] and LTK-03, Version Code 0103 [1, 2]; Firmware Version: 6.24.6 [1] and 6.24.7 [2]
3212	06/28/2018	NCoded Ultra Cryptographic Server Module	Ncoded Communications LLC	Software Version: 2.1
3213	06/28/2018	NCoded Ultra Cryptographic Mobile Module	Ncoded Communications LLC	Software Version: 2.1
3214	06/28/2018	Mocana Cryptographic Suite B Module	Mocana Corporation	Software Version: 6.5.1f
3215	06/29/2018	Oracle Linux 7 libgcrypt Cryptographic Module	Oracle Corporation	Software Version: R7-2.0.0