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 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: 12/5/2018

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 2018-12-05

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

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3317	11/01/2018	Forcepoint Next Generation Firewall	Forcepoint	Hardware Version: 1101, 2101, 2105, 3305, and 6205; Firmware Version: 6.4.1.20056.fips.8
3318	11/02/2018	BoringCrypto	Google, Inc.	Software Version: 66005f41fbc3529ffe8d007708756720529da20d
3319	11/05/2018	Juniper Networks SRX1500, SRX4100 and SRX4200 Services Gateways	Juniper Networks, Inc.	Hardware Version: SRX1500 SYS-JB-AC, SRX1500 SYS-JB-DC, SRX4100 SYS-JB-AC, SRX4100 SYS-JB-DC, SRX4200 SYS-JB-AC and SRX4200 SYS-JB-DC; with Tamper Seals JNPR-FIPS-TAMPER-LBLS; Firmware Version: Junos OS 17.4R1-S1
3320	11/06/2018	Splunk Phantom Cryptographic Module	Splunk, Inc.	Software Version: 1.0
3321	11/06/2018	Pitney Bowes X4 Hardware Security Module (HSM)	Pitney Bowes, Inc.	Hardware Version: Part # 4W84001 Rev AAA (MAX32590 Secure Microcontroller Revision B4); Firmware Version: Device Abstraction Layer (DAL) Version 01.01.0103; PB Bootloader Version 00.00.0016; HSM Application Version 21.01.0021
3322	11/06/2018	eToken 5300 Mini MD 4.3.5	Gemalto	Hardware Version: 214-010381-001: STM32F042K6U6TR [1] and SLE78CFX3000PH [2]; Firmware Version: 5300 FIPS FW ver-14.0.15 [1] and {IDCore30-revB - Build 06, IDPrime MD Applet version V4.3.5.D and MSPNP Applet V1.2} [2]
3323	11/07/2018	Trusted Platform Module ST33TPHF20SPI & ST33TPHF20I2C	STMicroelectronics	Hardware Version: ST33HTPH2E28AAF0 [1], ST33HTPH2E32AAF0 [1], ST33HTPH2E28AAF1 [1], ST33HTPH2E32AAF1 [1], ST33HTPH2028AAF3 [3], ST33HTPH2032AAF3 [3], ST33HTPH2E28AHB3 [1], ST33HTPH2E32AHB3 [1], ST33HTPH2E28AHB4 [1], ST33HTPH2E32AHB4 [1], ST33HTPH2E28AHB7 [2], ST33HTPH2E32AHB7 [2], ST33HTPH2E28AHB8 [2], ST33HTPH2E32AHB8 [2], ST33HTPH2028AHB9 [2], ST33HTPH2032AHB9 [2], ST33HTPH2E28AHC0 [1], ST33HTPH2E32AHC0 [1], ST33HTPH2028AHC1 [4], ST33HTPH2032AHC1 [4], ST33HTPH2E28AHC2 [2], ST33HTPH2E32AHC2 [2], ST33HTPH2028AHC3 [4] and ST33HTPH2032AHC3 [4]; Firmware Version: 49.08 [1], 49.09 [2], 4A.08 [3] and 4A.09 [4]
3324	11/08/2018	Samsung SAS 12G TCG Enterprise SSC SEDs PM163x Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILS920HCHP-000H9 [1, 2, 4], MZILS960HCHP-000H9 [1, 2, 4], MZILS1T9HCHP-000H9 [1, 2, 4], MZILS3T8HCJM-000H9 [1, 2, 4], MZILS400HCGR-000C6 [3], MZILS800HCHP-000C6 [3], MZILS1T6HCHP-000C6 [3] and MZILS3T2HCJM-000C6 [3]; Firmware Version: 3P00 [1], 3P02 [2], 3P03 [4] and EXP2 [3]
3325	11/10/2018	Bricata Cryptographic Module	Bricata, Inc.	Software Version: 2.2
3326	11/13/2018	Self-Defending Key Management Service(TM)	Fortanix, Inc.	Software Version: 2.0.596 and 2.0.NOAESNI-182

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3327	11/14/2018	SonicWALL TZ 300/TZ 300W, TZ 400/TZ 400W, TZ 500/TZ 500W, TZ 600, SOHOW, SM 9200, SM 9400, SM 9600 and NSâ, 2650, NSâ, 3600, NSâ, 3650, NSâ, 4600, NSâ, 4650, NSâ, 5600, NSâ, 5650, NSâ, 6600, NSâ, 6650, NSâ, 9250, NSâ, 9450, NSâ, 9650	SonicWall, Inc.	Hardware Version: 101-500403-55 Rev. F (TZ 300), 101-500404-54 Rev. E (TZ 300W), 101-500405-55 Rev. F (TZ 400), 101-500406-54 Rev. E (TZ 400W), 101-500411-56 Rev. G (TZ 500), 101-500412-55 Rev. F (TZ 500W), 101-500413-56 Rev. G (TZ 600), 101-500410-54 Rev. E (SOHOW), 101-500455-54 Rev. E (SM 9200), 101-500454-54 Rev. E (SM 9400), 101-500453-54 Rev. E (SM 9600), 101-500452-50 Rev. A (NSâ, 2650), 101-500459-54 Rev. E (NSâ, 3600), 101-500514-50 (NSâ, 3650), 101-500458-54 Rev. E (NSâ, 4600), 101-500451-50 (NSâ, 4650), 101-500457-54 Rev. E (NSâ, 5600), 101-500517-50 (NSâ, 5650), 101-500456-54 Rev. E (NSâ, 6600), 101-5005518-50 Rev A (NSâ, 6650), 101-500520-50 Rev A (NSâ, 9250), 101-500519-50 Rev A (NSâ, 9450), 101-500449-50 Rev A (NSâ, 9650); Firmware Version: SonicOS v6.5.2
3328	11/14/2018	CardioNet Cryptographic Module	CardioNet, Inc.	Software Version: 2.1
3329	11/20/2018	Cryptosec Dekaton	Realia Technologies, S.L.	Hardware Version: 1.1; Firmware Version: 12.11.3642
3330	11/21/2018	Infoblox Trinzic Virtual DDI Appliance	Infoblox	Firmware Version: NIOS 8.2.6
3331	11/21/2018	7705 SAR-OS SAR-A/M Cryptographic Module (SARCM)	Nokia Corporation	Software Version: SAR-OS Rel 8.0R6
3332	11/27/2018	Infoblox Trinzic 825, Trinzic 1425, Trinzic 2225, Trinzic 4015 and Trinzic 4025 DDI Appliances	Infoblox	Hardware Version: Trinzic 825 with Label Kit TE-805-FIPS, Trinzic 1425 with Label Kit TE-1405-FIPS, [Trinzic 2225, Trinzic 4015 and Trinzic 4025] with Label Kit TE-2205-FIPS; Firmware Version: NIOS 8.2.6
3333	11/28/2018	7705 SAR-OS SAR-18/8/X/Ax/Wx/W/H/Hc Control Plane Cryptographic Module (SARCPCM)	Nokia Corporation	Software Version: SAR-OS Rel 8.0R6
3334	11/29/2018	eToken 5300 Micro MD 4.3.5	Gemalto	Hardware Version: 214-010382-001: STM32F042K6U6TR [1] and SLE78CFX3000PH [2]; Firmware Version: 5300 FIPS FW ver-14.0.15 [1] and {IDCore30-revB - Build 06, IDPrime MD Applet version V4.3.5.D and MSPNP Applet V1.2} [2]