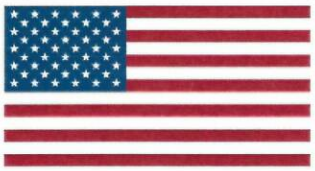
FIPS 140-2 Consolidated Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Canadian Centre for Cyber Security

May 2020

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, 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 COOPER Digitally signed by MICHAEL COOPER Date: 2020.07.07 09:32:23 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: June 16, 2020

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3650	05/06/2020	Trusted Platform Module ST33TPHF2XSPI [A], ST33TPHF2XI2C [B], ST33GTPMASPI [C] & ST33GTPMAI2C [D]	STMicroelectronics	Hardware Version: ST33HTPH revision A [A [1 and 2]], ST33HTPH revision A [B [3]], ST33G1M2A revision F [C [4]] and ST33G1M2A revision F [D [5]]; Firmware Version: 00.01.01.00 [1], 00.01.01.01 [2], 00.02.01.00 [3], 00.03.01.00 [4] and 00.06.01.00 [5]
3651	05/07/2020	Secure Kernel Code Integrity	Microsoft Corporation	Software Version: 10.0.17763
3652	05/08/2020	Amazon Linux 2 Libreswan Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
3653	05/18/2020	GigaVUE-HC2 Visibility Appliance	Gigamon Inc.	Hardware Version: GVS-HC201 and GVS-HC202 (Chassis) with SMT-HC0-X16 (GigaSMART), SMT-HC0-R (GigaSMART) and CTL-HC0-002 (Controller); FIPS Tamper Label SKU: ACC-HC0-FIPS; Firmware Version: 5.4.00.01
3654	05/19/2020	FortiGate-6301F/6501F	Fortinet, Inc.	Hardware Version: C1AG85, C1AG83 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: FortiOS 5.6, build4265,190820
3655	05/20/2020	RapidIdentity FIPS Cryptographic Module	Identity Automation	Software Version: 1.0
3656	05/20/2020	Cisco Catalyst 9800 Wireless Controllers running IOS-XE 16.10	Cisco Systems, Inc.	Hardware Version: 9800-40 and 9800-80; Firmware Version: IOS-XE 16.10
3657	05/26/2020	OpenSSL Cryptographic Module for Perimeta SBC	Metaswitch Networks Ltd	Software Version: 1.0
3658	05/26/2020	SonicWALL TZ 300/TZ 300W, TZ 300P, TZ 350/TZ 350W, TZ 400/TZ 400W, TZ 500/TZ 500W, TZ 600, TZ 600P, SOHO W, SOHO 250/SOHO 250W, SM 9200, SM 9400, SM 9600 and NSa 2650, NSa 3600, NSa 3650, NSa 4600, NSa 4650, NSa 5600, NSa 5650, NSa 6600, NSa 6650, NSa 9250, NSa 9450, NSa 9650	SonicWall, Inc.	Hardware Version: 101-500403-55 Rev. F (TZ 300), 101-500404-54 Rev. E (TZ 300W), 101-500582-52 Rev A (TZ 300P), 101-500622-52 Rev A (TZ 350), 101-500621-51 Rev A (TZ 350W), 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), 101-500581-51 Rev A (TZ 600P), 101-500410-54 Rev. E (SOHO W), 101-500624-51 Rev A (SOHO 250), 101-500623-52 Rev A (SOHO 250W), 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 (NSa 2650), 101-500459-54 Rev. E (NSa 3600), 101-500514-50 (NSa 3650), 101-500458-54 Rev. E (NSa 4600), 101-500451-50 (NSa 4650), 101-500457-54 Rev. E (NSa 5600), 101-500517-50 (NSa 5650), 101-500456-54 Rev. E (NSa 6600), 101-5005518-50 Rev A (NSa 6650), 101-500520-50 Rev A (NSa 9250), 101-500519-50 Rev A (NSa 9450), 101-500449-50 Rev A (NSa 9650); Firmware Version: SonicOS v6.5.4
3659	05/27/2020	Apricorn FIPS 140-2 Encryption System Gen 2	Apricorn	Hardware Version: P/Ns AFESG2-1 Rev A, AFESG2-2 Rev A, and AFESG2-3 Rev A; Firmware Version: 2.0
3660	05/27/2020	Barco ICMP	Barco n.v.	Hardware Version: R7681360-06; Firmware Version: 1.4.0.0.20979

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3661	05/29/2020	SafeZone FIPS Cryptographic Module	Rambus Global Inc., Finnish branch	Software Version: 1.2.0
3662	05/29/2020	Intel® DC SSD D7-D4512	Intel Corporation	Hardware Version: P/Ns SSDPD2KS019T8R with components J29722-003 Rev1 and J90877-300 Rev4, SSDPD2KS038T8R with components J29722-003 Rev1 and J90878-300 Rev4, SSDPD2KS076T8R with components J29722-003 Rev1 and J90879-300 Rev4 and SSDPD2KS153T8R with component J76794-100 Rev9; K33839-001 (Tamper-Evident Seals); Firmware Version: VPV1EF13
3663	05/29/2020	Cloudian cryptographic module	Cloudian, Inc.	Software Version: 1.0