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

June 2021

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: Timothy A. Hall

Dated: 10 July 2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____

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
3939	06/01/2021	Red Hat Enterprise Linux 7 Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190718
3940	06/01/2021	UD info DA-series FIPS SSD	UD info Corp.	Hardware Version: HF3-25DA128GB-A8P [A], HF3-25DA256GB-A8P [A], HF3-25DA512GB-A8P [A], HF3-25DA001TB-A8P [A], HF3-25DA002TB-A8P [A], M2S-80DA128GB-A8P [A], M2S-80DA256GB-A8P [A], M2S-80DA512GB-A8P [A], M2S-80DA001TB-A8P [A], M2S-80DA002TB-A8P [A], M2P-80DA256GB-A8P [B], M2P-80DA512GB-A8P [B], M2P-80DA001TB-A8P [B], M2P-80DA002TB-A8P [B]; Firmware Version: SCPU13.0 [A] and ECPU13.0 [B]
3941	06/02/2021	Broadcom FIPS Object Module for OpenSSL	Broadcom Inc.	Software Version: 1.0
3942	06/02/2021	FortiGate-6300F/6301F/6500F/6501F	Fortinet, Inc.	Hardware Version: FortiGate-6300F (C1AG83), FortiGate-6301F (C1AG85), FortiGate-6500F (C1AG84) and FortiGate-6501F (C1AG86) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.2 build 5547
3943	06/07/2021	Aegis Secure Key 3NX Cryptographic Module	Apricorn	Hardware Version: P/Ns ASK3NX-2GB, ASK3NX-4GB, ASK3NX-8GB, ASK3NX-16GB, ASK3NX-32GB, ASK3NX-64GB, ASK3NX-128GB, ASK3NXC-4GB, ASK3NXC-8GB, ASK3NXC-16GB, ASK3NXC-32GB, ASK3NXC-64GB, ASK3NXC-128GB; Hardware Version: Rev A3; Firmware Version: 1.8
3944	06/07/2021	Apricorn FIPS 140-2 Encryption System Gen 2	Apricorn	Hardware Version: P/Ns AFESG2-1 Rev A2, AFESG2-2 Rev A2 and AFESG2-3 Rev A2; Firmware Version: 2.1
3945	06/07/2021	VaultIP	Rambus Inc.	Hardware Version: 3.0.3; Firmware Version: 3.0.6
3946	06/07/2021	Red Hat Enterprise Linux 8 NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20200131
3947	06/07/2021	Astro Subscriber Motorola Advanced Crypto Engine (MACE) - Security Level 2	Motorola Solutions, Inc.	Hardware Version: P/Ns 5185912Y03, 5185912Y05 and 5185912T05; Firmware Version: R01.11.00 with [AES256 R01.00.00 and AES256 R02.00.00] and [ADP, DES-XL, DES, DVI-XL and/or DVP-XL R01.00.00]
3948	06/07/2021	Astro Subscriber Motorola Advanced Crypto Engine (MACE) - Security Level 3	Motorola Solutions, Inc.	Hardware Version: P/Ns 5185912Y03, 5185912Y05 and 5185912T05; Firmware Version: R01.11.00 with [AES256 R01.00.00 and AES256 R02.00.00] and [ADP, DES-XL, DES, DVI-XL and/or DVP-XL R01.00.00]
3949	06/07/2021	FAST C-LIB	Fescaro Co. Ltd.	Software Version: 1.0.0
3950	06/08/2021	Spectralink Cryptographic Module for BoringSSL	Spectralink	Software Version: 7f02881e96e51f1873afcf384d02f782b48967ca

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3951	06/08/2021	SQFlash FIPS Certified SSD	Advantech Co., Ltd.	Hardware Version: SQFFS25V2-128GSC [A], SQFFS25V4-256GSC [A], SQFFS25V8-512GSC [A], SQFFS25V8-1TSC [A], SQFFS25V8-2TSC [A], SQFFSM8V2-128GSC [A], SQFFSM8V4-256GSC [A], SQFFSM8V4-512GSC [A], SQFFSM8V4-1TSC [A], SQFFSM8V4-2TSC [A], SQFFCM8V4-256GEC [B], SQFFCM8V4-512GEC [B], SQFFCM8V4-1TEC [B], SQFFCM8V4-2TEC [B]; Firmware Version: SCPB13.0 [A] and ECPB13.0 [B]
3952	06/08/2021	WCC-PCN-AES100GB-F Encryption Module with FSP 3000 Shelf	ADVA Optical Networking SE	Hardware Version: 1063700027-01 version C-1.02 with one from [A] and one from [B]: Shelf P/Ns [A]: 1078700121 version 2.01, 1078700060-01 version 1.01, 1078700144 version 2.11 or 1078700145-01 version 1.01; CFP pluggable transceiver P/Ns [B]: 1061700617-01, 1061700618-01, 1061700618-02, 1061700619-01, 1061700619-02, 1061700630-01, 1061700634-01, or 1061700655-02; 1013700030-01, 1013700031-01 and 1013700032-01; Firmware Version: 172.19.7 or 193.1.7
3954	06/14/2021	Ubuntu 18.04 Google Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3955	06/14/2021	Acme Packet 4600 and Acme Packet 6300 and Acme Packet 6350	Oracle Communications	Hardware Version: 4600, 6300, 6350 with Dual NIU and 6350 with Quad NIU; Firmware Version: S-Cz8.4
3956	06/17/2021	Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20191106
3957	06/17/2021	SUSE Linux Enterprise Server GnuTLS Cryptographic Module	SUSE, LLC	Software Version: 1.0
3958	06/22/2021	Aruba AOS-CX Cryptographic Module	Aruba, a Hewlett Packard Enterprise company	Software Version: 1.0
3959	06/22/2021	Unisys Linux OpenSSL FIPS Object Module	Unisys Corporation	Software Version: 2.0
3960	06/27/2021	DocuSign HSM Appliance	DocuSign, Inc.	Hardware Version: 5.0; Firmware Version: 5.0.4
3961	06/29/2021	ST3H Ace Token	Securemetric Technology Sdn Bhd.	Hardware Version: ST3HAce-A1; Firmware Version: 1.0.11
3962	06/30/2021	SUSE Linux Enterprise Kernel Crypto API Cryptographic Module	SUSE, LLC	Software Version: 3.2
3963	06/30/2021	Envieta QFlex Hardware Security Module	Envieta Systems LLC	Hardware Version: 385HSM-FIPS Rev A and 385HSM-FIPS Rev B; Firmware Version: 1.3.0