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 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: 2020.07.15 14:38:21 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada Signature:

_____

Dated: July 3, 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
3664	06/01/2020	Ubuntu 18.04 AWS Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3667	06/04/2020	Deep Discovery Analyzer OpenSSL Cryptographic Module	TrendMicro Inc.	Software Version: 2.0.16
3668	06/11/2020	Juniper Networks MX204 3D Universal Edge Router and EX9251 Ethernet Switch	Juniper Networks, Inc.	Hardware Version: MX204 and EX9251; Firmware Version: Junos OS 19.2R1
3669	06/12/2020	FortiGate-5001E1 Blade with FortiGate-5144C Chassis	Fortinet, Inc.	Hardware Version: FortiGate-5001E1 (C1AG76), FortiGate-5144C (C1AB98), Blank Filler Panel - Front: (P16708-01): Thirteen, Blank Filler Panel - Rear (P16710-01): Fourteen, with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 5.6, build6022,190808
3670	06/16/2020	IDPrime 930 / 3930	Thales	Hardware Version: SLE78CFX400VPH - A1977038, SLE78CLFX400VPH - A1714221, SLE78CFX400VPH - A2023188 and SLE78CFX400VPH - A2410334; Firmware Version: IDCore3130 - Build 11D, IDPrime 930/3930 Applet V4.5 and MSPNP Applet V1.2
3671	06/16/2020	Infinera Cloud Xpress CX-1200F	Infinera	Hardware Version: Chassis Part Number (P/N): 800-1693-202; XMM2-S Controller Part Number (P/N): 130-2116-001; Firmware Version: IQC17.3
3672	06/18/2020	Anqlave v1.5 Module	Anqlave	Software Version: 1.5; Hardware Version: Intel Core i7-6600U
3673	06/22/2020	VMware's BC-FJA (Bouncy Castle FIPS Java API)	VMware, Inc.	Software Version: 1.0.2
3674	06/23/2020	FX Cryptographic Kernel Module for A57	Fuji Xerox Co., Ltd.	Software Version: 1.1.0