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

September 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 HALL Digitally signed by TIMOTHY HALL Date: 2021.10.07 08:52:30 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: October 6, 2021

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
4022	09/03/2021	NETSCOUT-FJA	NETSCOUT Systems Inc.	Software Version: 1.0.1
4023	09/07/2021	SBC 5400 Session Border Controller	Ribbon Communications, Inc.	Hardware Version: SBC 5400 with ASPEED AST2400 and FIPS Kit 550-06508; Firmware Version: R7.2.1R0
4024	09/07/2021	Splunk Cryptographic Module	Splunk Inc.	Software Version: 1.0
4025	09/09/2021	Intel(R) Offload and Crypto Subsystem (OCS)	Intel Corporation	Hardware Version: 4.0; Firmware Version: 15.0.20.1648
4026	09/13/2021	Cisco ISR 1000 Series Routers without MACSEC	Cisco Systems, Inc.	Hardware Version: ISR1101 and ISR1111; Firmware Version: IOS XE 16.9
4027	09/13/2021	Aqua OpenSSL Module	Aqua Security Software Ltd.	Software Version: 1.0
4028	09/13/2021	VMware's BoringCrypto Module	VMware, Inc.	Software Version: 3.0
4029	09/13/2021	Onclave FIPS Object Module for OpenSSL	Onclave Networks, Inc.	Software Version: 1.0
4030	09/13/2021	FortiGate-5001E1 Blade with FortiGate-5144C Chassis	Fortinet, Inc.	Hardware Version: FortiGate-5001E1 (C1AG76), FortiGate-5144C (C1AB98), Blank Filler Panel - Front (P16708-01), Blank Filler Panel - Rear (P16710-01) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548
4031	09/14/2021	Modius Cryptographic Security Module (MCSM)	Modius, Inc.	Software Version: 1.0.2.1
4032	09/17/2021	CliniComp Data Acquisition Cryptographic Module	CliniComp, Intl.	Software Version: cci-das-fips-crypto-1.0
4034	09/20/2021	Oracle Solaris Kernel Cryptographic Framework	Oracle Corporation	Software Version: 1.4
4035	09/21/2021	Trusted Key PKI Cryptographic Module	Mobile-ID Technologies And Services Joint Stock Company	Hardware Version: Trusted-Key-PKI-X15; Firmware Version: 1.0.11
4036	09/23/2021	Cisco FIPS Object Module	Cisco Systems, Inc.	Firmware Version: 7.2a
4037	09/24/2021	Ruckus Networks Virtual SmartZone - Data Plane (vSZ-D)	CommScope Technologies LLC	Software Version: 5.2.1.3
4038	09/27/2021	XSOC Cryptosystem	XSOC Corp	Software Version: 3.0.1