FIPS 140-2 Consolidated Validation Certificate

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

FIPS VALIDATED 140-2 TM

The Canadian Centre for Cyber Security

April 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 09:30:41 -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

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3639	04/02/2020	FortiOS 5.6	Fortinet, Inc.	Firmware Version: FortiOS 5.6, build6022,190808
3640	04/07/2020	Standalone IMB	GDC Technology (USA) LLC	Hardware Version: GDC-IMB-v5; Firmware Version: 4.0, Security Manager Firmware Version 1.8.0
3641	04/08/2020	GD Crypto Core Shared Library	General Dynamics Mission Systems	Software Version: 2.1.0
3642	04/20/2020	Leonovus Cryptographic Module	Leonovus Inc.	Software Version: 3.4
3643	04/20/2020	Amazon Linux 2 GnuTLS Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
3644	04/20/2020	Code Integrity	Microsoft Corporation	Software Version: 10.0.17763
3645	04/20/2020	QuantaNova Polymorphic Encryption Module - Mobile	QuantaNova	Software Version: 2.1
3646	04/20/2020	Amazon Linux 2 NSS Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
3647	04/24/2020	Ubuntu 18.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3648	04/29/2020	Ubuntu 18.04 Strongswan Cryptographic Module	Canonical Ltd.	Software Version: 2.0