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

March 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: 2020.04.23 10:08:49 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: April 17 2020

Manager, Product Assurance and Standards
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
3625	03/02/2020	Darktrace Cryptographic Module	Darktrace Limited	Software Version: 2.2
3626	03/02/2020	Veritas Cryptographic Module for Java	Veritas Technologies LLC	Software Version: 1.0
3627	03/03/2020	Verdasys Secure Cryptographic Module	Digital Guardian, Inc.	Software Version: 1.1
3628	03/04/2020	FortiProxy-400E/2000E/4000E	Fortinet, Inc.	Hardware Version: C1AG57, C1AD93 and C1AG58 with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiProxy 1.0, b0066, 190423
3629	03/04/2020	F5(R) Device Cryptographic Module	F5 Networks	Hardware Version: BIG-IP i4000, BIG-IP i5000, BIG-IP i5820-DF, BIG-IP i7000, BIG-IP i7820-DF, BIG-IP i10800, BIG-IP i11800-DS, BIG-IP i15800, BIG-IP 5250v-F, BIG-IP 7200v-F, BIG-IP 10200v-F, BIG-IP 10350v-F, VIPRION B2250, VIPRION B4450; Firmware Version: 14.1.0.3 EHF
3630	03/06/2020	Windows Embedded Compact Cryptographic Primitives Library (bcrypt.dll)	Microsoft Corporation	Software Version: 8.00.6273
3631	03/12/2020	Canon MFP Security Chip	Canon Inc.	Hardware Version: 3.0; Firmware Version: 3.00
3632	03/12/2020	Ubuntu 18.04 OpenSSH Server Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3633	03/12/2020	Ubuntu 18.04 OpenSSH Client Cryptographic Module	Canonical Ltd.	Software Version: 2.0
3634	03/20/2020	Orbit MCR and Orbit ECR	GE MDS LLC	Hardware Version: P/Ns MCR Chassis v1.0 and ECR Chassis v1.0; Component P/Ns: U91, L1B, L2X, L2B, L4A, L4E, L4C, L7A, L7W, L9C, 4G1, 4G2, 4G3, 4G4, 4G5, 4GP, 4GY, 4GZ, 4GA, E4S, E42, W51, W52, 3G1 and NNN (refer to Security Policy Tables 1 and 2 for valid combinations); Firmware Version: 7.1.1
3635	03/23/2020	Crown Sterling Cryptographic Module	Crown Sterling Limited, LLC	Software Version: 1.0
3636	03/23/2020	Oracle Cloud Infrastructure Cryptographic Library for Kubernetes	Oracle Corporation	Software Version: 1.0
3637	03/23/2020	ACT2Lite Cryptographic Module	Cisco Systems, Inc.	Hardware Version: 15-14497-02; Firmware Version: 1.5
3638	03/31/2020	Supermicro FIPS Object Module for OpenSSL	Super Micro Computer, Inc.	Software Version: 1.0