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

TM

February 2019

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 J Cooper

Dated: 3/7/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: March 7, 2019

Manager, Product Assurance and Standards
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 http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3356	02/02/2019	VMware's Linux Cryptographic Module	VMware, Inc.	Software Version: 2.0
3357	02/04/2019	Samsung NVMe TCG Opal SSC SEDs PM1723b Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLL3T8HAJQ-000G6; Firmware Version: NA01
3358	02/04/2019	Juniper Networks EX4300 Ethernet Switches	Juniper Networks, Inc.	Hardware Version: [EX4300-24P, EX4300-24T and EX4300-48T with component EX-UM-4X4SFP] and [EX4300-32F with component EX-UM-8X8SFP]; Firmware Version: Junos OS 17.4R1-S4
3359	02/04/2019	Samsung SAS 12G TCG Enterprise SSC SEDs PM1643 Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILT960HAHQ-000C9 [1], MZILT1T9HAJQ-000C9 [1], MZILT3T8HALS-000C9 [1], MZILT7T6HMLA-000C9 [2] and MZILT15THMLA-000C9 [2]; Firmware Version: EXF3[1] and EXV3[2]
3360	02/04/2019	RDX SATA III	Tandberg Data	Hardware Version: P/Ns 8812-RDX Version 3078-0006, 8813-RDX Version 3079-0006, 8815-RDX Version 3080-0006, 8816-RDX Version 3081-0006 and 8826 Version 3095-0003; 1022445 (FIPS Tamper-Evident Seals); Firmware Version: 0253
3361	02/04/2019	Titan Security Key, Chip Boundary	Google, Inc.	Hardware Version: H1B2; Firmware Version: 1.1
3362	02/05/2019	Security Builder® FIPS Module	Certicom Corp.	Software Version: 6.3.0
3363	02/06/2019	FortiMail-2000E/3000E	Fortinet, Inc.	Hardware Version: C1AD94 and C1AD97 with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiMail v6.0, build108,180731
3364	02/06/2019	Web Isolation Virtual Appliance	Symantec Corporation	Software Version: 1.10.48-fips+74
3365	02/06/2019	AgileSec FIPS Module	InfoSec Global Inc.	Software Version: 1.0
3366	02/07/2019	Proofpoint Cryptographic Module	Proofpoint Inc.	Software Version: 2.2
3367	02/08/2019	Juniper Networks QFX10002, QFX10008 and QFX10016	Juniper Networks, Inc.	Hardware Version: QFX10002-36Q, QFX10002-72Q and [QFX10008 and QFX10016 with QFX10000 Control board]; Firmware Version: Junos OS 18.1R1
3368	02/11/2019	Christie IMB-S3 4K Integrated Media Block (IMB)	Christie Digital Systems Canada Inc.	Hardware Version: 000-105081-03; Firmware Version: 2.1.4-4569
3369	02/11/2019	Cord3 Cryptographic Module	Cord3 Innovation Inc.	Software Version: 2.0.16
3370	02/12/2019	Juniper Networks MX240, MX480, MX960, MX2010, MX2020 3D Universal Edge Routers and EX9204, EX9208, EX9214 Ethernet Switches with RE-S-X6-64G/REMX2K-X8-64G/EX9200-RE2 Routing Engine	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208 and EX9214 with components identified in Security Policy Table 1; Firmware Version: Junos OS 18.1R1
3371	02/12/2019	Geotab Cryptographic Module	Geotab Inc.	Firmware Version: 1.0
3372	02/12/2019	Proofpoint Cryptographic Module for Java	Proofpoint Inc.	Software Version: 2.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3373	02/14/2019	GSP3000 Hardware Security Module	Futurex	Hardware Version: P/N 9800-2079 Rev7; Firmware Version: 6.2.0.3
3374	02/19/2019	IBM(R) z/VM(R) Version 6 Release 4 System SSL Cryptographic Module	IBM Corporation	Software Version: 5735FAL00: z/VM Version 6 Release 4 with 1701RSU and APAR PI99134; Hardware Version: z13 CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863
3375	02/19/2019	Zebra Inline Crypto Engine (SDCC)	Zebra Technologies Corporation	Hardware Version: 3.0.0
3376	02/19/2019	Zebra Pseudo Random Number Generator	Zebra Technologies Corporation	Hardware Version: 2.3.1
3377	02/19/2019	Zebra Crypto Engine Core	Zebra Technologies Corporation	Hardware Version: 5.3.4
3378	02/19/2019	Unbound Tech EKM Cryptographic Module	Unbound Tech	Software Version: 2.0
3379	02/21/2019	Juniper Networks MX240, MX480, MX960, MX2010, and MX2020 3D Universal Edge Routers with RE-S-X6-64G/REMX2K-X8-64G Routing Engine and Multiservices MPC	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960, MX2010 and MX2020 with components identified in Security Policy Table 1; Firmware Version: Junos OS 18.1R1
3380	02/21/2019	FortiMail 6.0	Fortinet, Inc.	Firmware Version: FortiMail v6.0, build108,180731
3381	02/26/2019	CipherLoc Polymorphic Encryption Core	CipherLoc Corporation	Software Version: 1.0
3385	02/28/2019	IBM(R) FlashSystem(TM) 9100 NVMe FlashCore(TM) Module	IBM(R) Corporation	Hardware Version: 01EK231, 01EK232, 01EK233; Firmware Version: 1.3.0.91
3386	02/28/2019	Juniper Networks MX240, MX480, MX960, MX2010, and MX2020 3D Universal Edge Routers with RE1800 Routing Engine and Multiservices MPC	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960, MX2010 and MX2020 with components identified in Security Policy Table 1; Firmware Version: Junos OS 17.4R1-S1