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

January 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 J Cooper
Dated: 2/6/2020
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature: ____________
Dated: Feb 04 2020
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
3588	01/02/2020	Unity/Unity XT 12 Gb/s SAS I/O Module with Encryption	Dell EMC	Hardware Version: Storage Processor SAS Module with P/N 362-000-332, P/N 363-000-071, P/N 363-000-084 and P/N 364-000-096 [1], Embedded SAS Module with P/N 362-000-333, P/N 363-000-071, P/N 363-000-084 and P/N 364-000-096 [2] and Pluggable I/O SAS Module with P/N 362-000-333, P/N 363-000-071, P/N 363-000-084 and P/N 364-000-063 [1 or 2]; Firmware Version: 03.90 [1] and 04.10 [2]
3589	01/02/2020	AKEYLESS FIPS Cryptographic Module for Distributed Fragments Cryptography	AKEYLESS Security Ltd	Software Version: 1.0
3590	01/06/2020	Oracle Linux 7 OpenSSH Server Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
3591	01/06/2020	Cisco Catalyst 9500 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst C9500-32C, Cisco Catalyst C9500-32QC, Cisco Catalyst C9500-48YC, Cisco Catalyst C9500-24YC, Cisco Catalyst C9500-24Q, Cisco Catalyst C9500-12Q, Cisco Catalyst C9500-40X and Cisco Catalyst C9500-16X with components C9500-NM-8X and C9500-NM-2Q; Firmware Version: Cisco IOS-XE 16.9.2
3592	01/06/2020	Postal NRevenector US 2018	FP InovoLabs GmbH	Hardware Version: 58.0036.0301.00 and 58.0036.0302.00; Firmware Version: Bootloader 90.0036.0401.00/2019141001 and US Application 90.0036.0416.00/2019141001
3593	01/07/2020	STOP 8 Kernel Cryptographic Module	BAE Systems	Software Version: 1.2.1
3594	01/07/2020	Key Management Security Module (KMSM) Cryptographic Module	KeyNexus, Inc.	Software Version: 1.0
3595	01/08/2020	Raytheon Cryptographic Module	Raytheon Company	Software Version: 2.2
3596	01/09/2020	Cryptographic Module for BIG-IP (R)	F5 Networks	Software Version: 14.1.0.3
3597	01/10/2020	SonicWALL SMA Series v12.1 SMA 6210, SMA 7210	SonicWall, Inc.	Hardware Version: SMA 6210 [P/N 101-500564-50] and SMA 7210 [P/N 101-500563-50]; Firmware Version: 12.1.0-05887
3598	01/10/2020	KMF/Wave/Traffic CryptR	Motorola Solutions, Inc.	Hardware Version: P/Ns CLN8566A, Rev. 0x1 and CLN1875A, Rev. 0x1; Firmware Version: R03.03.05 with or without AES128 R01.00.01, AES256 R01.00.03, and/or ADP/DES-XL/DES-OFB/DES-ECB/DES-CBC/DVI-XL/DVP-XL/Localized Capable R01.00.00
3599	01/10/2020	Cisco Catalyst 9300 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9300-24T, Cisco Catalyst 9300-24P, Cisco Catalyst 9300-24U, Cisco Catalyst 9300-24UX, Cisco Catalyst 9300-48T, Cisco Catalyst 9300-48P, Cisco Catalyst 9300-48U, Cisco Catalyst 9300-48UX and Cisco Catalyst 9300-48UN; Firmware Version: Cisco IOS-XE 16.9.2

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3600	01/13/2020	Network Security Platform Sensor NS7150, NS7250 and NS7350	McAfee, LLC	Hardware Version: P/Ns IPS-NS7150 Version 1.00, IPS-NS7250 Version 1.00 and IPS-NS7350 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 9.1.17.100
3601	01/14/2020	µMACE	Motorola Solutions, Inc.	Hardware Version: P/N 51009730001, Rev 0x0001; Firmware Version: R03.01.12 with or without AES128 R01.00.01, AES256 R01.00.03, and/or ADP/DES-XL/DES-OFB/DES-ECB/DES-CBC/DVI-XL/DVP-XL/Localized Capable R01.00.00
3602	01/17/2020	HYP2003 Cryptographic Module	Hypersecu Information Systems Inc	Hardware Version: HYP2003-A3 and HYP2003-X15; Firmware Version: 1.0.11
3603	01/17/2020	Aegis Fortress L3 Cryptographic Module	Apricorn	Hardware Version: P/Ns AFL3-500, AFL3-1TB, AFL3-2TB, AFL3-3TB, AFL3-4TB, AFL3-5TB, AFL3-S500, AFL3-S1TB, AFL3-S2TB, AFL3-S4TB, AFL3-S8TB, and AFL3-S16TB; Hardware Version: Rev A; Firmware Version: 3.1
3604	01/21/2020	Oracle Linux 7 libgcrypt Cryptographic Module	Oracle Corporation	Software Version: R7-4.0.0
3605	01/22/2020	TMC TCG OPAL SSC Self-Encrypting Solid State Drive CD5 Series	Toshiba Memory Corporation	Hardware Version: A2 with KCD5FLUG960G, A2 with KCD5FLUG1T92, A2 with KCD5FLUG3T84 and A2 with KCD5FLUG7T68; Firmware Version: KCD50107
3606	01/22/2020	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.4
3607	01/23/2020	Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers and EX9204, EX9208, EX9214 Ethernet Switches with RE-S-X6-64G/RE-S-X6-128G/EX9200-RE2 Routing Engine and MPC7E-10G/EX9200-40XS MACSec Card	Juniper Networks, Inc.	Hardware Version: MX240, MX480, MX960, EX9204, EX9208, EX9214 with components identified in Security Policy Table 1; Firmware Version: Junos OS 18.3R1-S1
3608	01/24/2020	Wickr FIPS Object Module for OpenSSL	Wickr Inc.	Software Version: 2.0.16
3609	01/24/2020	Raytheon Cryptographic Module for Java	Raytheon Company	Software Version: 3.0.1
3610	01/24/2020	Thales Advanced Security Platform (TASP)	Thales Group	Hardware Version: TASP 1.0, P/N: SUB00116-00-03 Version K; Firmware Version: U-Boot Version 1.1.22
3611	01/28/2020	RSA BSAFE(R) Crypto-J JSAFE and JCE Software Module	RSA	Software Version: 6.2 [1], 6.2.1.1 [2] and 6.2.1.2 [3]
3612	01/29/2020	Samsung NVMe TCG Opal SSC SEDs PM1723b Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLL1T9HAJQ-000H9, MZWLL3T8HAJQ-000H9, MZWLL7T6HMLA-000H9, MZWLL15THMLA-000H9; Firmware Version: P101
3613	01/31/2020	Trend Micro NSS Crypto Module	Trend Micro, Inc.	Software Version: 4.0