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 2022

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: 2022.04.06 10:36:48 -04'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: April 6 2022

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
4166	03/01/2022	Keysight Technologies Cryptographic Module for OpenSSL	Keysight Technologies	Software Version: 1.0
4167	03/01/2022	DINAMO CD, XP, and ST Hardware Security Modules	DINAMO Networks, Inc.	Hardware Version: DINAMO CD, DINAMO XP and DINAMO ST; Firmware Version: 5.0.8.0
4168	03/01/2022	Command Encryption Module	Mitsubishi Space Software Co., Ltd.	Hardware Version: Tamper Evident Seal Part Number: MSS-FIPS-19-500; Firmware Version: 4.0
4169	03/04/2022	Oracle Linux 7 Unbreakable Enterprise Kernel (UEK 6) Cryptographic Module	Oracle Corporation	Software Version: R7-7.8.0
4170	03/04/2022	Oracle Linux 7 OpenSSL Cryptographic Module	Oracle Corporation	Software Version: R7-7.8.0
4171	03/04/2022	Oracle Linux 7 NSS Cryptographic Module	Oracle Corporation	Software Version: R7-7.8.0
4172	03/07/2022	RSA BSAFE(R) Crypto Module	Dell Australia Pty Limited, BSAFE Product Team	Software Version: 1.1
4173	03/08/2022	Motorola Solutions Cryptographic Firmware Module	Motorola Solutions, Inc.	Firmware Version: R01.09.01 and R01.11.00
4174	03/09/2022	Cisco FIPS Object Module	Cisco Systems, Inc.	Software Version: 7.0b
4175	03/13/2022	Octopus Authentication Server Cryptographic Module	Secret Double Octopus	Software Version: 1.0
4176	03/14/2022	Oracle Linux 7 OpenSSH Server Cryptographic Module	Oracle Corporation	Software Version: R7-7.8.0
4177	03/15/2022	AWS Key Management Service HSM	Amazon Web Services, Inc.	Hardware Version: 2.0; Firmware Version: 1.6.109, 1.6.163 and 1.6.165
4178	03/15/2022	Cellcrypt Core V4 FIPS 140-2 Module	Cellcrypt	Software Version: CCoreV4
4179	03/15/2022	ProtectServer Internal Express 2 (PSI-E2)	Thales	Hardware Version: 808-000064-005; Firmware Version: 5.06.01 with bootloader version 1.1.2
4180	03/20/2022	Qualcomm(R) Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.6.2
4181	03/20/2022	Qualcomm(R) Crypto Engine Core	Spectralink Corporation	Hardware Version: 5.3.4
4182	03/21/2022	N-able Cryptographic Module	N-able Technologies Inc.	Software Version: 2.2
4183	03/22/2022	Hitachi Virtual Storage Platform (VSP) Encryption Module	Hitachi, Ltd.	Hardware Version: P/N: 3289094-A(BS12GE) Version: B/D4, B/D5, B/D4a, B/D5a, B/D6, B/D7, B/D8, B/D10 ,B/D13; P/N: 3292522-A(BS12GE) Version: D/D10, D/D11, D/D12, D/D13; P/N: 3293600-A(BS12GE) Version: F/D11, F/D13; P/N: 3293418-A(BS12GE) Version: B/B1; Firmware Version: 03.09.34.00

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4184	03/24/2022	Adaptiva Edge Platform Cryptographic Module	Adaptiva	Software Version: 1.0.2.1, 1.0.2.2 and 1.0.2.3
4185	03/26/2022	OSNEXUS Crypto Library	OSNEXUS Corporation	Software Version: 1.0
4186	03/28/2022	Cigent Secure SSD Advanced FIPS M.2 2280	Cigent Technology Inc.	Hardware Version: CGN-110050IF, CGN-110100IF and CGN-110200IF; Firmware Version: ECPM13.1
4187	03/29/2022	Aviat Networks Eclipse Cryptographic Module	Aviat Networks, Inc.	Hardware Version: INUe 2RU Chassis (P/N EXE-002), Fan Card (P/N EXF-101), Node Controller Card (P/N EXN-004 with FPGA_NCCV2_E1_DS1_004.bit and FPGA_NCCV2_STM1_006.bit), Node Controller Card V3 (P/N EXN-005 with FPGA_NCCV3_E1_DS1_010.bit and FPGA_NCCV3_STM1_033.bit), FIPS Installation Kit (P/N 179-530153-001 or 179-530153-002), Replacement Seals (P/N 007-600331-001), at least one of: [RAC 6X (P/N EXR-600-001 with FPGA_RAC6X_PDH_ACM-14.28.33.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 6XE (P/N EXR-600-002 with FPGA_RAC6X_PDH_ACM-14.28.33.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 60 (P/N EXR-660-001 with FPGA_RAC6X_PDH_ACM-14.28.33.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 60E (P/N EXR-660-002 with FPGA_RAC6X_PDH_ACM-14.28.33.bit and FPGA_RAC6X_SDH-2.3.1.bit), RAC 70 (P/N EXR-700-001 with FPGA_RAC7X_PDH_ACM-2.32.77.bit), RAC 70 V2 (P/N EXR-700-002 with FPGA_RAC7X_PDH_ACM-2.32.77.bit), RAC 7X (P/N EXR-770-001 with FPGA_RAC7X_PDH_ADM-2.32.77.bit) or RAC 7X V2 (P/N EXR-770-002 with FPGA_RAC7X_PDH_ACM-2.32.77.bit)] and all remaining slots filled by excluded components as specified in the Security Policy; Firmware Version: 08.13.95 with Bootloader version 1.0.36
4188	03/29/2022	TruLink Control Logic Module CL6792-M1	Telephonics Corporation	Hardware Version: P/N 010.6792-01 Rev. H3; Firmware Version: Boot: SW7098 v2.6 and Application: SW7099 v9.20
4189	03/29/2022	TruLink Control Logic Module CL6882-M1	Telephonics Corporation	Hardware Version: P/N 010.6882-01 Rev. B2; Firmware Version: Boot: SW7158 v2.5 and Application: SW7151 v2.13