

FIPS 140 Series Consolidated Validation Certificate



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



The Canadian Centre for Cyber Security

February 2025

The National Institute of Standards and Technology, as the United States FIPS 140 Series Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140 Series Cryptographic Module Validation Authority; hereby validate the FIPS 140 Series testing results of the cryptographic modules listed below. The FIPS 140 Series specify 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 the FIPS 140 Series 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.

The FIPS 140 Series 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 the areas of a cryptographic module that are related to its secure design and implementation.

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: _____

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____

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

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4957	02/05/2025	Tellabs Optical LAN OLT Cryptographic Module	Tellabs Enterprise, Inc.	Software Version: 2.1.2
4958	02/06/2025	Tellabs Panorama PON Manager Cryptographic Module	Tellabs Enterprise, Inc.	Software Version: 3.0.2.1
4959	02/07/2025	Juniper Networks EX4300-48MP Ethernet Switch	Juniper Networks, Inc.	Hardware Version: EX4300-48MP; Firmware Version: Junos OS 22.4R2.8
4960	02/07/2025	Juniper Networks PTX1000 Packet Transport Router	Juniper Networks, Inc.	Hardware Version: PTX1000; Firmware Version: Junos OS 22.4R2.8
4961	02/07/2025	Juniper Networks PTX10008 and PTX10016 Packet Transport Routers	Juniper Networks, Inc.	Hardware Version: [PTX10008 and PTX10016 with components Routing Engine JNP10K-RE0, MACsec Line Card LC1105-M]; Firmware Version: Junos OS 22.4R2.8
4962	02/07/2025	Thales Luna G7 Cryptographic Module	Thales	Hardware Version: 808-000080-001, 808-000080-002, 808-000064-005, 808-000064-006; Firmware Version: 7.7.3 with bootloader versions 1.3.0, 1.5.0 and 1.6.0
4963	02/10/2025	Edge Security Cryptographic Module	Ultra Intelligence and Communications	Hardware Version: 1.0; Firmware Version: 1.0
4964	02/12/2025	Byos OpenSSL FIPS Provider	Byos Inc.	Software Version: 3.0.9
4965	02/13/2025	Samsung TCG Opal SSC Cryptographic Sub-Chip	Samsung Electronics Co., Ltd.	Hardware Version: S01; Firmware Version: SS0100
4966	02/14/2025	Cisco Adaptive Security Appliance Cryptographic Module (FPR 3100 Series)	Cisco Systems, Inc.	Hardware Version: [FPR 3105, FPR 3110, FPR 3120, FPR 3130 and FPR 3140] with FIPS Kits (AIR-AP-FIPSKIT= and FPR3K-FIPS-KIT=); Firmware Version: 9.20.1
4967	02/19/2025	Dell BSAFE™ Crypto Module for C	Dell Australia Pty Limited, BSAFE Product Team	Software Version: 3.0.1
4968	02/20/2025	SUSE Rancher Kubernetes Cryptographic Library	SUSE LLC	
4969	02/21/2025	Gloo BoringCrypto	Solo.io	
4970	02/25/2025	Honeywell Mobility Edge™ Boring Crypto	Honeywell International Inc.	
4971	02/24/2025	Amazon Linux 2023 Libgcrypt Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.10.2-752a14d13e4ce9c0
4972	02/26/2025	AN/KRC-6 (ATCS-BBU)	Ultra Intelligence & Communications	Hardware Version: AN/KRC-6(v)1; Firmware Version: 1.1.1
4973	02/26/2025	VMware's BoringCrypto Module	Broadcom Inc.	
4974	02/26/2025	SE Cryptographic Library	Schneider Electric IT Corporation	
4975	02/27/2025	Certes Java Cryptographic Module	Certes Networks, Inc.	

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4976	02/27/2025	Keeper Security Cryptographic Module v2	Keeper Security, Inc.	
4977	02/27/2025	Copeland TempTrak Java Crypto Library	Copeland, LP	
4978	02/27/2025	Motorola Solutions Advanced Crypto Engine (MACE) HSM – Security Level 3	Motorola Solutions, Inc.	Hardware Version: P/N 5185912T05; Firmware Version: R04.01.04 with [AES128 R01.00.05 and AES256 R01.00.07]
4979	02/28/2025	Cisco Secure Firewall Threat Defense Cryptographic Module (FPR 3100 Series)	Cisco Systems, Inc.	Hardware Version: [FPR 3105, FPR 3110, FPR 3120, FPR 3130 and FPR 3140] with FIPS Kits (AIR-AP-FIPSKIT= and FPR3K-FIPS-KIT=); Firmware Version: 7.4.0