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

August 2026

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: DAVID HAWES Digitally signed by DAVID HAWES Date: 2026.09.24 07:08:43 -04'00'

Dated: _____

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Lau, Hedy Digitally signed by Lau, Hedy Date: 2026.09.23 08:56:42 -04'00'

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
5399	08/14/2026	Junos® OS Evolved Kernel Cryptographic Module	Juniper Networks, Inc.	
5404	08/31/2026	Boot Manager	Microsoft Corporation	
5405	08/31/2026	Windows OS Loader	Microsoft Corporation	
5406	08/20/2026	Code Integrity	Microsoft Corporation	
5407	08/20/2026	Secure Kernel Code Integrity	Microsoft Corporation	
5408	08/31/2026	Kernel Mode Cryptographic Primitives Library	Microsoft Corporation	
5409	08/31/2026	BitLocker Dump Filter	Microsoft Corporation	
5410	08/31/2026	Cryptographic Primitives Library	Microsoft Corporation	
5459	08/04/2026	Forescout FIPS module for Java	Forescout Technologies	Software Version: 4.0.0
5460	08/05/2026	Virtru Go Cryptographic Module	Virtru Corporation	
5461	08/05/2026	Red Hat Enterprise Linux 8 Kernel Cryptographic API	Red Hat, LLC	
5462	08/05/2026	Arista MACsec data plane accelerator [on-chip]	Arista Networks, Inc.	
5463	08/05/2026	VaultIC408 1.2.4	SEALSQ	
5464	08/05/2026	SUSE Linux Enterprise Libica Cryptographic Module	SUSE LLC	
5465	08/05/2026	Port Authority Series	Communication Devices Inc.	
5466	08/06/2026	Juniper Networks NFX150 and NFX250 Network Services Platform	Juniper Networks, Inc.	
5467	08/06/2026	Qualcomm® Crypto Engine Core	Qualcomm Technologies, Inc.	
5468	08/06/2026	WildFire 10.2 WF-500 and WF-500-B	Palo Alto Networks Inc.	
5469	08/06/2026	Qualcomm® Pseudo Random Number Generator	Qualcomm Technologies, Inc.	
5470	08/06/2026	Junos® OS Evolved Kernel Cryptographic Module version 2.1	HPE Juniper Networking	
5471	08/06/2026	Motorola Solutions Advanced Crypto Engine (MACE) HSM - Security Level 3	Motorola Solutions, Inc.	
5472	08/06/2026	Cisco ASA FX-OS on 4K/9K Cryptographic Module	Cisco Systems, Inc.	

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
5473	08/07/2026	Ruckus Networks Virtual SmartZone - Data Plane (vSZ-D)	Ruckus Wireless LLC	
5474	08/11/2026	Knuckle Cryptographic Module	Google, Inc.	
5475	08/11/2026	HP Inc. OpenSSL FIPS Provider based on the OpenSSL FIPS Provider	HP Inc.	
5476	08/11/2026	Amazon Linux 2023 GnuTLS Cryptographic Module	Amazon Web Services, Inc.	
5477	08/11/2026	VaultIC408 1.2.4 - Level 2	SEALSQ	
5478	08/11/2026	Arista MACsec data plane accelerator [on-chip-driver]	Arista Networks, Inc.	
5479	08/12/2026	DB Series SSD Drives	UD info Corp.	
5480	08/12/2026	Palo Alto Networks SD-WAN Instant-On Network (ION) Devices ION 1200, ION 1200-S, ION 3200, ION 3200H, ION 5200, and ION 9200	Palo Alto Networks, Inc.	
5481	08/12/2026	FortiGate 7.2 and 7.4	Fortinet, Inc.	
5482	08/13/2026	OpenSSL FIPS Provider for AlmaLinux 9	Cloudlinux Inc., TuxCare division	
5483	08/13/2026	Ultrastar DC HC560 TCG Enterprise HDD, SED and Ultrastar DC HC570 TCG Enterprise HDD, SED	Western Digital Technologies, Inc.	
5484	08/14/2026	GlobalProtect App	Palo Alto Networks	
5485	08/14/2026	Microsoft HSM Cryptographic Module	Microsoft Corporation	
5486	08/14/2026	IBM® Crypto for C	IBM Corporation	
5487	08/14/2026	Cryptographic Module for BIG-IP	F5, Inc.	
5488	08/16/2026	MonoCrypt AES Enhanced Crypto Library	Focus Systems Corporation	
5489	08/17/2026	Juniper Express 4 MACsec Cryptographic Module	Juniper Networks, Inc.	
5490	08/17/2026	Junos® OS Evolved MACsec Cryptographic Library	Juniper Networks, Inc.	

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
5491	08/17/2026	Canonical Ltd. Ubuntu 22.04 Kernel Crypto API Cryptographic Module	Canonical Ltd.	
5492	08/17/2026	Motorola Solutions Advanced Crypto Engine (MACE) HSM - Security Level 2	Motorola Solutions, Inc.	
5493	08/17/2026	FortiClient Crypto Module v1.0	Fortinet Inc.	
5494	08/18/2026	Geotab Extended Cryptographic Module	Geotab Inc.	
5495	08/18/2026	Seagate SSG3 TCG Enterprise SSC SED FIPS 140 Module	Seagate Technology LLC	
5496	08/18/2026	Rocky Linux 9 GnuTLS Cryptographic Module	Ctrl IQ, Inc.	
5497	08/19/2026	QASM Cryptographic Module	Crypto4A Technologies Inc.	
5498	08/19/2026	Aviat Networks Eclipse Cryptographic Module	Aviat Networks, Inc.	
5499	08/21/2026	Phison PASCARI X and D-series NVMe TCG OPAL SSC Self-Encrypting Enterprise SSD	Phison Electronics Corporation	
5500	08/24/2026	Palo Alto Networks SD-WAN Virtual Instant-On Network (vION)	Palo Alto Networks, Inc.	
5502	08/25/2026	Marvell LS2 HSM Family	Marvell Semiconductor, Inc.	
5503	08/25/2026	Sansec HSM Cryptographic Module	Sansec Technology Co., Ltd.	
5504	08/25/2026	Qualcomm® Pseudo Random Number Generator	Qualcomm Technologies, Inc.	
5505	08/25/2026	F5OS-A Cryptographic Module	F5, Inc.	
5506	08/27/2026	BlueCat Networks Cryptographic Module	BlueCat Networks	
5507	08/27/2026	Bitwarden Cryptographic Module	Bitwarden, Inc.	
5508	08/31/2026	Ciena Waveserver Ai WCS-2	Ciena Corporation	