

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

September 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 Digitally signed by DAVID
HAWES
Dated: HAWES Date: 2026.10.13 15:06:18
-04'00'

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall Digitally signed by King, Lyall
Date: 2026.10.09 10:52:08
-04'00'

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
5509	09/01/2026	HPE Juniper Networking QFX5120-48YM	HPE Juniper Networking	
5510	09/01/2026	Supermicro FIPS Provider for OpenSSL	Super Micro Computer, Inc.	
5511	09/02/2026	HiPKI SafGuard 2000 HSM	Chunghwa Telecom laboratories	
5512	09/03/2026	Dell BSAFE™ Crypto Module for C	Dell Australia Pty Limited, BSAFE Product Team	
5513	09/08/2026	Red Hat Enterprise Linux 8 NSS Cryptographic Module	Red Hat, Inc.	
5514	09/08/2026	SUSE Linux Enterprise NSS Cryptographic Module	SUSE LLC	
5515	09/08/2026	Arista WiFi Access Points	Arista Networks, Inc.	
5516	09/09/2026	Astro Subscriber Motorola Advanced Crypto Engine (MACE) - Security Level 3	Motorola Solutions, Inc.	
5517	09/09/2026	Aegis Secure Key 3.0 Cryptographic Module	Apricorn	
5518	09/10/2026	PTP 700 Point to Point Wireless Ethernet Bridge	Cambium Networks, Ltd.	
5519	09/11/2026	Motorola BoringCrypto Android 14	Motorola Mobility Inc	
5520	09/11/2026	Motorola BoringCrypto Android 15	Motorola Mobility Inc	
5521	09/11/2026	Samsung BoringCrypto Android 14	Samsung Electronics Co., Ltd.	
5522	09/14/2026	Micron® MSA11-P5 Controller Sub Chip Security Subsystem	Micron Technology, Inc.	
5523	09/15/2026	Chainguard FIPS Provider for OpenSSL	Chainguard, Inc.	
5524	09/16/2026	Barracuda FIPS Provider based on the OpenSSL FIPS Provider	Barracuda Networks, Inc.	
5525	09/16/2026	CryptoComply Module based on AWS-LC FIPS	SafeLogic, Inc.	
5526	09/17/2026	TW-900-F/950-F TSM Shadow, TW-880-F TSM Ghost Embedded, TW-870-F/875-F TSM Ghost, TW-135-F TSM Shadow High-Power	TrellisWare Technologies, Inc.	

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
5527	09/18/2026	Loadbalancer.org FIPS Object Module based on the OpenSSL FIPS Provider	Loadbalancer.org Ltd	
5528	09/20/2026	G&D Cryptographic Module	Guntermann & Drunck GmbH	
5529	09/22/2026	Junos® OS Evolved Juniper Express 5 MACsec Cryptographic Module Version 1.0	HPE Juniper Networking	
5530	09/23/2026	Samsung BoringCrypto Android 15	Samsung Electronics Co., Ltd.	
5531	09/24/2026	Astro Subscriber Motorola Advanced Crypto Engine (MACE) - Security Level 2	Motorola Solutions, Inc.	
5532	09/28/2026	IDPrime PIV 4.0 FIDO on IDCore3230 Platform	Thales	
5533	09/28/2026	MolecuLightDX Cryptographic Module	MolecuLight Inc.	
5534	09/28/2026	Qualcomm® Inline Crypto Engine (UFS)	Qualcomm Technologies, Inc.	
5535	09/29/2026	HPE Aruba Networking VIA Cryptographic Module	Hewlett Packard Enterprise	
5536	09/30/2026	Harris AES Load Module	L3Harris Technologies, Inc.	