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

October 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

Dated: Date: 2026.11.05 13:58:07 -05'00'

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

Dated: Date: 2026.11.04 15:19:05 -05'00'

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

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
5537	10/01/2026	Google Tensor 6th Gen UFS Inline Storage Encryption Engine	Google LLC	
5538	10/05/2026	Infinera Groove G30 Cryptographic Module	Infinera Corporation (Nokia)	
5539	10/05/2026	B227 True Random Number Generator (TRNG) Cryptographic Module	Google, LLC	
5540	10/05/2026	WaveLogic 5 Extreme Encryption Modem	Ciena Corporation	
5541	10/05/2026	Waveserver 5 Control Processor Module	Ciena Corporation	
5542	10/06/2026	InformaCast Advanced and Reach Server C Crypto Library	Singlewire Software, LLC	
5543	10/06/2026	AudioCodes BoringCrypto	AudioCodes Ltd.	
5544	10/07/2026	TW-860-F TSM Spirit	TrellisWare Technologies, Inc.	
5545	10/07/2026	Skydio Cryptographic Module (based on BoringCrypto)	Skydio, Inc.	
5546	10/07/2026	Crypto Module for Intel® Core Ultra Series 1 (Meteor Lake) Converged Security and Manageability Engine (CSME)	Intel Corporation	
5547	10/09/2026	Qualcomm® Crypto Engine Core	Qualcomm Technologies, Inc.	
5548	10/09/2026	wolfCrypt	wolfSSL Inc.	
5549	10/09/2026	Motorola P25 KVL 7000 HSM	Motorola Solutions Inc.	
5550	10/10/2026	Integrated Compute Complex (ICC)	Google, LLC	
5551	10/15/2026	Cisco FTD FX-OS on 4K/9K Cryptographic Module	Cisco Systems, Inc.	
5552	10/16/2026	Seagate SSG5 TCG Enterprise SSC SED FIPS 140 Module	Seagate Technology LLC.	
5553	10/19/2026	Qualcomm® Crypto Engine Core	Qualcomm Technologies, Inc.	
5554	10/19/2026	Qualcomm® Crypto Engine Core	Qualcomm Technologies, Inc.	
5555	10/19/2026	Fortanix DSM Appliance	Fortanix, Inc.	
5556	10/19/2026	RA8M1 Security Management Module	Renesas Electronics Corporation	
5557	10/20/2026	Echo FIPS Provider for Java	Echo Software Inc.	Software Version: 4.0.0
5558	10/20/2026	Integrated Compute Complex (ICC)	Google, LLC	

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
5559	10/20/2026	Micron® MTC22-P4 Controller Sub Chip Security Subsystem	Micron Technology, Inc.	
5560	10/21/2026	Echo FIPS Provider for OpenSSL	Echo Software Inc.	
5561	10/21/2026	Ad Noctem Connect 2.3	Northrop Grumman Corporation	
5562	10/25/2026	Ergotron Cryptographic Module	Ergotron, Inc.	
5563	10/29/2026	FortiGate-VM 7.2/7.4	Fortinet, Inc.	
5564	10/29/2026	FortiOS 7.2/7.4	Fortinet, Inc.	
5565	10/30/2026	Inline Crypto Engine (ICE)	Google, LLC	
5566	10/30/2026	TM400ENB	ECI Telecom Ltd / Ribbon communications Operating company, Inc.	