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

December 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: 2023.01.05 09:16:27 -05'00'

Dated: _____

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 DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall" Reason: I am approving this document Location: Date: 2023.01.04 09:13:54-05'00' Foxit PDF Editor Version: 12.1.0

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
4383	12/03/2022	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.6
4384	12/05/2022	Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20210614
4385	12/06/2022	Fortress Mesh Points	General Dynamics Mission Systems	Hardware Version: ES2440, ES520v1, ES520v2 and ES820; Firmware Version: 5.4.7
4386	12/07/2022	Apacer TCG SSD SV240 Series	Apacer Technology Inc.	Hardware Version: A12.A25HGF[B], A12.A25HHF[D], A12.A22HGF[A], A12.A22HHF[C], A12.A25JGF[B], A12.A25JHF[D], A12.A22JGF[A], A12.A22JHF[C], A12.A25KGF[B], A12.A25KHF[D], A12.A22KGF[A], A12.A22KHF[C], A12.A25LGF[B], A12.A25LHF[D], A12.A23AGF[A], A12.A23AHF[C], A12.A25MGF[B], A12.A25MHF[D], A12.A23BGF[A], A12.A23BHF[C], A92.A25HGA[B], A92.A25HHA[D], A92.A22HGA[A], A92.A22HHA[C], A92.A25JGA[B], A92.A25JHA[D], A92.A22JGA[A], A92.A22JHA[C], A92.A25KGA[B], A92.A25KHA[D], A92.A22KGA[A], A92.A22KHA[C], A92.A25LGA[B], A92.A25LHA[D], A92.A23AGA[A], A92.A23AHA[C], A72.A25HGA[B], A72.A25HHA[D], A72.A22HGA[A], A72.A22HHA[C], A72.A25JGA[B], A72.A25JHA[D], A72.A22JGA[A], A72.A22JHA[C], A72.A25KGA[B], A72.A25KHA[D], A72.A22KGA[A], A72.A22KHA[C], A72.A25LGA[B], A72.A25LHA[D], A72.A23AGA[A], A72.A23AHA[C], A72.A25MGA[B], A72.A25MHA[D], A72.A23BGA[A], A72.A23BHA[C], A52.A25HGB[B], A52.A25HHB[D], A52.A22HGB[A], A52.A22HHB[C], A52.A25JGB[B], A52.A25JHB[D], A52.A22JGB[A], A52.A22JHB[C], A52.A25KGB[B], A52.A25KHB[D], A52.A22KGB[A], A52.A22KHB[C], A52.A25LGB[B], A52.A25LHB[D], A52.A23AGB[A], A52.A23AHB[C], A52.A25MGB[B], A52.A25MHB[D], A52.A23BGB[A], A52.A23BHB[C] with tamper-evident labels 40.09134.0200C; Firmware Version: SFYCA01S[A], SFYCA11S[B], SFYCA21S[C], SFYCA31S[D]
4387	12/07/2022	Juniper Networks MX2010 and MX2020 3D Universal Edge Routers with REMX2K-X8-64G and RE-MX2000-1800X4-S Routing Engines, MPC9E with MIC-MACSEC-MRATE	Juniper Networks, Inc.	Hardware Version: MX2010 and MX2020 with components identified in Security Policy Table 1; Firmware Version: Junos OS 20.3X75
4388	12/07/2022	DIGIPASS GO7	OneSpan	Hardware Version: DIGIPASS GO7 FIPS140-2; Firmware Version: 340106
4389	12/07/2022	Apple corecrypto Module v11.1 [Intel, User, Software]	Apple Inc.	Software Version: 11.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4390	12/07/2022	Apple corecrypto Module v11.1 [Intel, Kernel, Software]	Apple Inc.	Software Version: 11.1
4391	12/07/2022	Apple corecrypto Module v11.1 [Apple silicon, User, Software]	Apple Inc.	Software Version: 11.1
4392	12/07/2022	Apple corecrypto Module v11.1 [Apple silicon, Kernel, Software]	Apple Inc.	Software Version: 11.1
4393	12/15/2022	Vocera Cryptographic Module	Vocera Communications, Inc.	Firmware Version: 6.0
4394	12/15/2022	Blue Armor Cryptographic Module	Blue Armor	Software Version: 2.2.1
4395	12/16/2022	CRATON2/SECTON embedded V2X HSM	Autotalks Ltd.	Hardware Version: P/N ATK66610, Version 2.1.2; Firmware Version: 3.0
4396	12/20/2022	Ruckus Wireless Cloudpath Enrollment System Cryptographic Library	CommScope Technologies LLC	Software Version: 5.10
4397	12/20/2022	Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20200615
4398	12/22/2022	Seagate Secure(R) TCG Enterprise SSC Self-Encrypting Drives FIPS 140 Module	Seagate Technology LLC	Hardware Version: ST2000NX0333[1], ST2000NX0353[2]; Firmware Version: KF06[1], EF06[2]

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4399	12/27/2022	NITROXIII CNN35XX-NFBE HSM Family	Marvell	Hardware Version: P/Ns CNL3560P-NFBE-G, CNL3560-NFBE-G, CNL3530-NFBE-G, CNL3510-NFBE-G, CNL3510P-NFBE-G, CNN3560P-NFBE-G, CNN3560-NFBE-G, CNN3530-NFBE-G, CNN3510-NFBE-G, Version HW-1.0; CNL3560P-NFBE-2.0-G, CNL3560-NFBE-2.0-G, CNL3530-NFBE-2.0-G, CNL3510-NFBE-2.0-G, CNL3510P-NFBE-2.0-G, CNN3560P-NFBE-2.0-G, CNN3560-NFBE-2.0-G, CNN3530-NFBE-2.0-G, CNN3510-NFBE-2.0-G, CNL3560B-NFBE-2.0-G, CNL3530B-NFBE-2.0-G, CNN3510LP-NFBE-2.0-G, CNN3510LPB-NFBE-2.0-G, CNN3505LP-NFBE-2.0-G, Version HW-2.0; CNL3560P-NFBE-3.0-G, CNL3560-NFBE-3.0-G, CNL3560B-NFBE-3.0-G, CNL3560A-NFBE-3.0-G, CNL3560C-NFBE-3.0-G, CNL3560D-NFBE-3.0-G, CNL3560E-NFBE-3.0-G, CNL3560F-NFBE-3.0-G, CNL3510P-NFBE-3.0-G, CNL3510A-NFBE-3.0-G, CNL3510C-NFBE-3.0-G, CNL3510D-NFBE-3.0-G, CNL3510E-NFBE-3.0-G, CNL3510F-NFBE-3.0-G, CNL3530-NFBE-3.0-G, CNL3530B-NFBE-3.0-G, CNL3530A-NFBE-3.0-G, CNL3530C-NFBE-3.0-G, CNL3530D-NFBE-3.0-G, CNL3530E-NFBE-3.0-G, CNL3530F-NFBE-3.0-G, CNL3510-NFBE-3.0-G, CNL3510I-NFBE-3.0-G, CNL3530I-NFBE-3.0-G, CNL3560I-NFBE-3.0-G, CNN3560P-NFBE-3.0-G, CNN3560-NFBE-3.0-G, CNN3560A-NFBE-3.0-G, CNN3560C-NFBE-3.0-G, CNN3560D-NFBE-3.0-G, CNN3560E-NFBE-3.0-G, CNN3560F-NFBE-3.0-G, CNN3530-NFBE-3.0-G, CNN3530A-NFBE-3.0-G, CNN3530C-NFBE-3.0-G, CNN3530D-NFBE-3.0-G, CNN3530E-NFBE-3.0-G, CNN3530F-NFBE-3.0-G, CNN3510-NFBE-3.0-G, CNN3510A-NFBE-3.0-G, CNN3510C-NFBE-3.0-G, CNN3510D-NFBE-3.0-G, CNN3510E-NFBE-3.0-G, CNN3510F-NFBE-3.0-G, CNN3510LP-NFBE-3.0-G, CNN3510LPB-NFBE-3.0-G, CNN3510LPA-NFBE-3.0-G, CNN3510LPC-NFBE-3.0-G, CNN3510LPD-NFBE-3.0-G, CNN3510LPE-NFBE-3.0-G, CNN3510LPF-NFBE-3.0-G, CNN3505LP-NFBE-3.0-G, CNN3505LPA-NFBE-3.0-G, CNN3505LPC-NFBE-3.0-G, CNN3505LPD-NFBE-3.0-G, CNN3505LPE-NFBE-3.0-G and CNN3505LPF-NFBE-3.0-G, Version HW-3.0; Firmware Version: CNN35XX-NFBE-FW-3.4 build 10
4400	12/27/2022	Integrated Management Complex (IMC) and B227 True Random Number Generator (TRNG) Firmware-Hybrid Cryptographic Module	Google, LLC	Hardware Version: 3.00b; Firmware Version: 20220318
4401	12/30/2022	AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor	Advanced Micro Devices (AMD)	Hardware Version: bc0c0140FIPS001; Firmware Version: bc0c0140FIPS001
4402	12/30/2022	AMD Ryzen PRO 4000 Series PSP Cryptographic CoProcessor	Advanced Micro Devices (AMD)	Hardware Version: bc0c0042FIPS001; Firmware Version: bc0c0042FIPS001