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

May 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: 2022.06.10 08:39:53 -04'00'

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 with my legally binding signature Location: your signing location here Date: 2022.06.07 14:02:08-04'00' Foxit PDF Editor Version: 11.2.1

Dated: _____

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4210	05/04/2022	Titaniam Core Engine	Titaniam, Inc.	Software Version: 1.0
4211	05/04/2022	Oracle Linux 8 Unbreakable Enterprise Kernel (UEK6) Cryptographic Module	Oracle Corporation	Software Version: R8-8.4.0
4212	05/05/2022	Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module	Google, LLC	Hardware Version: 2.3.1
4213	05/06/2022	DHSSL Cryptographic Module	Zhejiang Dahua Technology Co., Ltd.	Software Version: 1.0.0
4214	05/09/2022	Juniper Kernel Crypto Cryptographic Module	Juniper Networks, Inc.	Software Version: 1.0
4215	05/09/2022	Oracle Linux 8 OpenSSL Cryptographic Module	Oracle Corporation	Software Version: R8-8.4.0
4216	05/09/2022	Samsung BoringSSL Android	Samsung Electronics Co., Ltd.	Software Version: 1.6
4217	05/09/2022	Nokia BC-FJA (Bouncy Castle FIPS Java API)	NOKIA SOLUTIONS AND NETWORKS OY	Software Version: 1.0.2.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4218	05/09/2022	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 and 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, CNL3560PB-NFBE-2.0-G, CNL3560B-NFBE-2.0-G, CNL3530B-NFBE-2.0-G, CNL3510B-NFBE-2.0-G, CNL3510PB-NFBE-2.0-G, CNN3510LP-NFBE-2.0-G, CNN3510LPB-NFBE-2.0-G, CNN3560P-NFBE-2.0-G, CNN3560-NFBE-2.0-G, CNN3530-NFBE-2.0-G, CNN3510-NFBE-2.0-G and CNN3505LP-NFBE-2.0-G, Version HW-2.0; CNL3560P-NFBE-3.0-G, CNL3560B-NFBE-3.0-G, CNL3560-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, CNL3560I-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, CNL3530I-NFBE-3.0-G, CNL3510-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, CNL3510I-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-2.06 build 15
4219	05/09/2022	Secure Cryptographic Module (SCM)	JVCKENWOOD Corporation	Hardware Version: P/N KWD-AE30, Versions 2.0.0, 2.1.0 and 2.2.0; Firmware Version: A3.0.1, A3.0.2, A3.0.3, A3.0.4 and A3.1.0
4220	05/09/2022	McAfee Core Cryptographic Module (kernel)	Trellix	Software Version: 2.1.0.41
4221	05/09/2022	McAfee Core Cryptographic Module (user)	Trellix	Software Version: 2.1.0.41 [1] or 2.1.0.(b41.1) [2]
4222	05/09/2022	IOS Common Cryptographic Module (IC2M)	Cisco Systems, Inc.	Firmware Version: Rel5a

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4223	05/10/2022	7705 SAR-OS SAR-18/8/X/Ax/Wx/W/H/Hc Data Plane Cryptographic Module (SARDCM)	Nokia Corporation	Hardware Version: SAR-8, SAR-18, SAR-Ax, SAR-H, SAR-Hc, SAR-W, SAR-Wx, SAR-X; Firmware Version: SAR-OS 20.4 R3.
4224	05/10/2022	Virtual PSD Module	Quadient, Inc.	Hardware Version: N/A; Firmware Version: IBM FW Segment 1: 5.3.19 P0130 M0130 P0130 F0D01 Partial Hash = E2157B6F IBM FW Segment 2: 5.3.23 Toolkit Development Partial Hash = F0B7 1A25 3731 and Neopost Segment 3: NeopostUDX Version: 2.0.3-21-06-02-Release-ee523cf0bd19dd6378c7f9fbe931cbd5b83316e7
4225	05/12/2022	X4i Hardware Security Module (HSM)	Pitney Bowes, Inc.	Hardware Version: MAX32590 Secure Microcontroller Revision B4; Firmware Version: PB Bootloader Version 00.00.0016, HSM Application Version 21.04.0008, and Device Abstraction Layer (DAL) Version 01.02.002F
4226	05/12/2022	Oracle Linux 8 NSS Cryptographic Module	Oracle Corporation	Software Version: R8-8.4.0
4227	05/16/2022	Alaris™ PC Unit Model 8015	BD	Hardware Version: Model 8015 b/g, Model 8015 a/b/g, Model 8015 a/b/g/n or BD Alaris Model 8015 a/b/g/n with FIPS Kit 49000550; Firmware Version: 12.1.2
4228	05/16/2022	Defender HDD 300	Kanguru Solutions	Hardware Version: KDH300-CM Version 2.0; Firmware Version: V01.06.0000.0000
4229	05/16/2022	Oracle Linux 8 GnuTLS Cryptographic Module	Oracle Corporation	Software Version: R8-8.4.0
4230	05/16/2022	Ranger Cryptographic Module	Tavve Holdings, LLC	Software Version: 1.0.2.1, 1.0.2.2 and 1.0.2.3
4231	05/23/2022	7705 SAR-OS SAR-A/M Cryptographic Module (SARCM)	Nokia Corporation	Software Version: SAR-OS 20.4R3
4232	05/23/2022	Oracle Linux 8 libgcrypt Cryptographic Module	Oracle Corporation	Software Version: R8-8.4.0
4233	05/24/2022	VMware's Linux Cryptographic Module	VMware, Inc.	Software Version: v4.0.1
4234	05/24/2022	ICU Medical CE3.0 OpenSSL Cryptographic Module	ICU Medical, Inc.	Software Version: 2.0.9.1
4235	05/25/2022	Huawei EulerOS 2.0 OpenSSL Cryptographic Module	Huawei Technologies CO., Ltd.	Software Version: 1.1
4236	05/25/2022	NEC Storage Encryption Board for SAS	NEC Corporation	Hardware Version: P/N: 3293418-A(BS12GE) Version: B/B1; Firmware Version: 03.09.34.00
4237	05/25/2022	Panzura CloudFS (TM) FIPS Cryptographic Module	Panzura	Software Version: 1.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4238	05/26/2022	Samsung NVMe TCG Opal SSC SEDs PM1733/PM1735 Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLR1T9HBJR-00AD9, MZWLR3T8HBLS-00AD9, MZWLR7T6HALA-00AD9, MZWLR1T6HBJR-00AD9, MZWLR3T2HBLS-00AD9, MZWLR6T4HALA-00AD9, MZWLR12THALA-00AD9, MZWLR15THALA-00AD9; Firmware Version: MPK92D3Q, MPK95D3Q
4239	05/31/2022	Hitachi Vantara Cryptographic Library	Hitachi Vantara, LLC	Software Version: 1.0.2.3