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

April 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: 2022.05.03 14:56:53 -04'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Mullen, Michele

Dated: 05/03/2022

Director General, Partnership and Risk Mitigation
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
4190	04/04/2022	SecureDoc® Cryptographic Engine for Windows	WinMagic Corp	Software Version: 8.7
4191	04/04/2022	HyTrust KeyControl Cryptographic Module	HyTrust, Inc.	Software Version: 1.1
4192	04/07/2022	SecureDoc® Cryptographic Engine for macOS/Linux	WinMagic Corp	Software Version: 8.7
4193	04/11/2022	STAR-2000	JoveAI Innovation, Inc.	Hardware Version: JV00002-02-1B-5 [1] and JV00002-02-1B-C [2]; Firmware Version: 1.0.1.1 [1] and 1.1.1.1 [2]
4194	04/11/2022	Hitachi Virtual Storage Platform (VSP) Encryption Board for NVMe	Hitachi, Ltd.	Hardware Version: P/N:VSPEBN-001 Version: 001; Firmware Version: FPGA Main Firmware Ver : ED00802E; FPGA Configuration data Ver : ED000002_19112100 or ED000101_20120700; FPGA bootloader Firmware Ver: 00000003
4195	04/14/2022	Thales Luna Backup HSM Cryptographic Module	Thales	Hardware Version: 808-000064-005, 808-000064-006; Firmware Version: 7.7.1 and bootloader version 1.3.0 or 1.5.0
4196	04/14/2022	RAD X-1040 AES-256	Vcinity, Inc.	Hardware Version: RAD X-1040 (90-0206-101) Rev L; Firmware Version: RAD X Release 4.0.1
4197	04/18/2022	RSA BSAFE(R) Crypto-C Micro Edition	Dell Inc, BSAFE Product Team	Software Version: 4.1.4
4198	04/21/2022	Summit Linux FIPS Core Crypto Module	Laird Connectivity	Software Version: 7.1
4199	04/21/2022	Voice Processing Module Cryptographic Module (VPMCM) / Telephone Media Gateway Cryptographic Module (TMGCM)	Motorola Solutions, Inc.	Hardware Version: P/Ns VPMCRYPTO_B or VPMCRYPTO_C; Firmware Version: R01.13.01 with AES256 R01.00.00
4200	04/21/2022	NCoded Ultra Cryptographic Mobile Module	NCoded Communications, Inc.	Software Version: 2.1
4201	04/22/2022	ZBR-88W8887-WLAN	Zebra Technologies Corporation	Hardware Version: P/N: NXP 88W8887 (Version 1.0); Firmware Version: NXP Firmware Version 15.68.19.p59 and Zebra 8887 FIPS Driver Firmware Version 2.0
4202	04/22/2022	IQVIA Java Crypto Module	IQVIA	Software Version: 1.0
4203	04/22/2022	Monaco Communication Cryptographic Module 1.0	Monaco Enterprises Inc.	Hardware Version: 314R0006; Firmware Version: 51.01
4204	04/25/2022	7705 SAR-OS SAR-18/8/X/Ax/Wx/W/H/Hc Control Plane Cryptographic Module (SARCM)	Nokia Corporation	Software Version: SAR-OS 20.4 R3

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4205	04/27/2022	NEC Storage Encryption Board for NVMe	NEC Corporation	Hardware Version: P/N:VSPEBN-001 Version: 001; Firmware Version: FPGA Main Firmware Ver : ED00802E; FPGA Configuration data Ver : ED000101_20120700; FPGA bootloader Firmware Ver: 00000003
4206	04/29/2022	Oracle Linux 7 OpenSSH Client Cryptographic Module	Oracle Corporation	Software Version: R7-7.8.0
4207	04/29/2022	Ultrastar® DC HC310 TCG Enterprise HDD, Ultrastar® DC HC320 TCG Enterprise HDD, and Ultrastar® DC HC330 TCG Enterprise HDD	Western Digital Corporation	Software Version: N/A; Hardware Version: P/Ns HUS726T4TAL5205 [4], HUS726T4TALS205 [4], HUS726T6TAL5205 [4], HUS728T8TAL5205 [3] and WUS721010AL5205 [1, 2, 3, 5, 6] (Operational Tested); Firmware Version: R920 [1], R942 [2], R980 [3], R984 [4], NA00 [5], and NE00 [6]
4208	04/29/2022	CN Series Encryptors	Senetas Corporation Ltd., distributed by Thales SA (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. & SafeNet Inc. CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Senetas Corp. Ltd. & Thales CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. & Thales CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. & Thales CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Firmware Version: 5.2.0
4209	04/29/2022	CN6000 Series Encryptors	Senetas Corporation Ltd., distributed by Thales SA (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & Thales CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Firmware Version: 5.2.0