

# 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

**February 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: \_\_\_\_\_

Dated: \_\_\_\_\_

Chief, Computer Security Division  
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: \_\_\_\_\_

Dated: March 2 2022

Director, Risk Mitigation Programs  
Canadian Centre for Cyber Security

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4142	02/02/2022	Oracle Solaris Userland Cryptographic Framework	Oracle Corporation	Software Version: 1.4
4143	02/03/2022	Samsung NVMe TCG Opal SSC SEDs PM1733 Series	Samsung Electronics Co., Ltd.	Hardware Version: MZWLJ1T9HBJR-000H9, MZWLJ1T9HBJR-00AH9, MZWLJ3T8HBLS-000H9, MZWLJ3T8HBLS-00AH9, MZWLJ7T6HALA-000H9, MZWLJ7T6HALA-00AH9, MZWLJ15THALA-000H9 and MZWLJ15THALA-00AH9; Firmware Version: 3P00
4144	02/03/2022	NetApp CryptoMod	NetApp, Inc.	Software Version: v2.2
4145	02/07/2022	Hewlett Packard Enterprise libgcrypt Crypto Module	Hewlett Packard Enterprise	Software Version: 5.0
4146	02/07/2022	Cloudera Cryptographic Module for NSS	Cloudera, Inc.	Software Version: 5.0
4147	02/09/2022	Hewlett Packard Enterprise NSS Crypto Module	Hewlett Packard Enterprise	Software Version: 5.0
4148	02/09/2022	Cloudera Cryptographic Module for Libgcrypt	Cloudera, Inc.	Software Version: 5.0
4149	02/10/2022	CHR Cryptographic Module	Atos	Hardware Version: 006/D; Firmware Version: V1.06-03L
4150	02/10/2022	Intel(R) Converged Security and Manageability Engine (CSME) Crypto Module for Tiger Point PCH, Mule Creek Canyon PCH, and Rocket Lake PCH	Intel Corporation	Hardware Version: 4.0; Firmware Version: 15.0.20.1648[1], 15.0.30.1716[2], 15.0.22.1571[3] and 15.40.10.2204[4]
4151	02/10/2022	u.trust Anchor	Utimaco IS GmbH	Hardware Version: Hardware P/N u.trust Anchor Version 7.03.0.3; Firmware Version: Device System v1.17.4 and Sensory Controller v3.02.0.7
4152	02/14/2022	i.MX 8X SECO HSMv2	NXP Semiconductors	Hardware Version: P/N: rpp_cm0p_sec_subsys (version tag DA_SSL_iMX8QX_SCU_SUBSYS_LN28FDSOI_1.72); Firmware Version: ROM mem_i.MX8QX_s28roml_w20480x032m32B2_1Tlms_m0_1.3; SECO FW 4.8.0
4153	02/14/2022	Cryptographic Server HSM	Beijing Lianshi Networks Technology Co.,Ltd.	Hardware Version: CS-HSM-2697v2-680-32G; Firmware Version: 1.1.0.1
4154	02/15/2022	Sansec HSM Cryptographic Module	Sansec Technology Co., Ltd.	Hardware Version: SecHSM V2-1 (AC) and SecHSM V2-1 (DC); Firmware Version: v3.02.0025
4155	02/15/2022	TW-900/950 TSM Shadow and TW-870/875 TSM Ghost	TrellisWare Technologies, Inc.	Hardware Version: ASY0750164 Rev.C, ASY0750090 Rev.C, ASY0750203 Rev.B, ASY0750220 Rev.B with FIPS kit TrellisWare P/N 800AAA0036; Firmware Version: 6.1.6-fips-b2
4156	02/16/2022	BoringCrypto Android	Google, LLC.	Software Version: dcdc7bbc6e59ac0123407a9dc4d1f43dd0d117cd
4157	02/16/2022	Tactical Key Management Device (TKMD)	Christine Wireless, Inc.	Hardware Version: TKMD Spin 3; Firmware Version: TKMD_FIPS_FINAL_11_01_20

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4158	02/17/2022	Cryptographic Module for Intel(R) Converged Security and Manageability Engine (CSME)	Intel Corporation	Hardware Version: 3.0; Firmware Version: 12.0.70.1652
4159	02/17/2022	WatchKey ProX USB Token Cryptographic Module	WatchData Technologies Pte Ltd	Hardware Version: Smart Card Chip AS518 and K023314A; Firmware Version: 36410102
4160	02/22/2022	Emerson TempTrak Crypto Module	Emerson Digital Cold Chain	Software Version: 1.0.2.1, 1.0.2.2 and 1.0.2.3
4161	02/22/2022	SonicWALL NSsp 14700 and NSsp 15700	SonicWall, Inc.	Hardware Version: 101-500645-50 (NSsp 14700), 101-500639-52 (NSsp 15700); Firmware Version: SonicOSX 7.0
4162	02/22/2022	SonicWALL TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700 and NSa 3700	SonicWall, Inc.	Hardware Version: 101-500665-50 (TZ270), 101-500666-50 (TZ270W), 101-500649-50 (TZ370), 101-500648-50 (TZ370W), 101-500643-50 (TZ470), 101-500629-50 (TZ470W), 101-500594-51 (TZ570), 101-500593-51 (TZ570W), 101-500640-50 (TZ570P), 101-500592-51 (TZ670), 101-500661-50 (NSa 2700), 101-500663-50 (NSa 3700); Firmware Version: SonicOS 7.0
4163	02/22/2022	CryptoComply for HSM	SafeLogic Inc.	Hardware Version: 808-000048-002, 808-000066-001, 808-000073-001; Boot Loader: 1.1.1, 1.1.2, 1.1.4; Firmware Version: 7.0.1, 7.0.2, 7.0.3, 7.3.3
4164	02/24/2022	Trend Micro NSS Crypto Module	Trend Micro Inc.	Software Version: 5.0
4165	02/28/2022	Splunk Cryptographic Module	Splunk Inc.	Software Version: 2.2