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

October 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: 2022.11.07 17:46:42 -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: your signing location here Date: 2022.11.07 10:35:45-05'00' 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
4312	10/03/2022	GM01	Shanghai Muge Technology Co., Ltd	Hardware Version: 1.0.0; Firmware Version: 1.0.0
4313	10/04/2022	Cloudera Cryptographic Module for Java	Cloudera, Inc.	Software Version: 3.0.2.1
4314	10/04/2022	Poly Crypto Module for Java	Plantronics, Inc.	Software Version: 3.0.2.1
4315	10/04/2022	Veritas Cryptographic Module for Java	Veritas Technologies LLC	Software Version: 3.0.2.1
4316	10/04/2022	InformaCast Java Crypto Library	Singlewire Software	Software Version: 3.0.2.1
4317	10/04/2022	Saviynt Cryptographic Module	Saviynt	Software Version: 3.0.2.1
4318	10/04/2022	CTERA Crypto Module(TM) (Java)	CTERA Networks Ltd.	Software Version: 3.0.2.1
4319	10/04/2022	Raytheon Cryptographic Module for Java	Raytheon Technologies	Software Version: 3.0.2.1
4320	10/05/2022	SR-OS Cryptographic Module	Nokia Corporation	Firmware Version: 20.10R4
4321	10/06/2022	Dell Crypto Library for Dell iDRAC and Dell OME-M	Dell, Inc.	Software Version: 2.6
4322	10/06/2022	Qualcomm(R) Trusted Execution Environment (TEE) Software Cryptographic Library	Qualcomm Technologies, Inc.	Software Version: 5.13-00023; Hardware Version: Snapdragon(R) 8cx Gen 3 Mobile Compute Platform
4324	10/10/2022	CyberCogs Hardware Security Module	CyberCogs, Inc.	Hardware Version: CC50-3, CC100-3, CC200-3, CC300-3, CC400-3, CC50-4, CC100-4, CC200-4, CC300-4 and CC400-4; Firmware Version: 3.0
4325	10/10/2022	CryptoManager Root of Trust (CMRT)	Rambus Inc.	Hardware Version: 0x60000611; Firmware Version: 2022-02-21-gd74d034
4327	10/12/2022	Thales Cryptovisor K7 Cryptographic Module	Thales	Hardware Version: 808-000048-002, 808-000048-003, 808-000073-001 and 808-000073-002; Firmware Version: 2.0.0 with Boot Loader versions 1.1.1, 1.1.2, 1.1.4 and 1.1.5
4328	10/12/2022	Thales Cryptovisor K7+ Cryptographic Module	Thales	Hardware Version: 808-000069-001 and 808-000070-001; Firmware Version: 2.0.0 with Boot Loader versions 1.1.1, 1.1.2, 1.1.4 and 1.1.5
4329	10/12/2022	3e-636 CyberFence Cryptographic Module	Ultra Intelligence and Communications	Hardware Version: 1.0; Firmware Version: 5.2
4330	10/14/2022	CS67PLUS Cryptographic Module	Comtech Systems, Inc.	Hardware Version: 004F014840-1
4331	10/16/2022	MiniHSM & MiniHSM for nShield Edge F2	Entrust	Hardware Version: nC4031Z-10 and nC3021U-10, Build Standard N; Firmware Version: 12.72.0
4332	10/16/2022	MiniHSM & MiniHSM for nShield Edge F3	Entrust	Hardware Version: nC4031Z-10 and nC4031U-10, Build Standard N; Firmware Version: 12.72.0
4333	10/16/2022	nShield Solo XC F2	Entrust	Hardware Version: nC3025E-000, Build Standard A; Firmware Version: 12.72.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4334	10/16/2022	nShield Solo XC F3 & nShield Solo XC F3 for nShield Connect XC and for nShield HSMi	Entrust	Hardware Version: nC4035E-000 and nC4335N-000, Build Standard A; Firmware Version: 12.72.1
4335	10/16/2022	nShield Solo XC F3 & nShield Solo XC F3 for nShield Connect XC and for nShield HSMi	Entrust	Hardware Version: nC4035E-000 and nC4335N-000, Build Standard A; Firmware Version: 12.72.1
4336	10/16/2022	nShield F2 500+ & nShield F2 1500+ & nShield F2 6000+	Entrust	Hardware Version: nC3423E-500, nC3423E-1K5 and nC3423E-6K0, Build Standard N; Firmware Version: 12.72.0
4337	10/16/2022	nShield F3 10+ 500+ 6000+ & nShield F3 500+ 1500+ 6000+ for nShield Connect+, Connect CLX and HSMi	Entrust	Hardware Version: nC4033E-010, nC4433E-500, nC4433E-6K0, nC4433E-500N, nC4433E-1K5N and nC4433E-6K0N, Build Standard N; Firmware Version: 12.72.0
4338	10/16/2022	nShield F3 10+ 500+ 6000+ & nShield F3 500+ 1500+ 6000+ for nShield Connect+, Connect CLX and HSMi	Entrust	Hardware Version: nC4033E-010, nC4433E-500, nC4433E-6K0, nC4433E-500N, nC4433E-1K5N and nC4433E-6K0N, Build Standard N; Firmware Version: 12.72.0
4339	10/17/2022	Windows OS Loader	Microsoft Corporation	Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3]
4346	10/24/2022	Vocality RoIP and DTECH M3-SE Multi-Function Gateway Appliances	Cubic Corporation	Hardware Version: Vocality RoIP and DTECH M3-SE Multi-Function Gateway; Firmware Version: 5.0.1
4347	10/24/2022	Trusted Platform Module 2.0 SLB 9672	Infineon Technologies AG	Hardware Version: SLB 9672VU20 (Package PG-UQFN-32-1 or PG-UQFN-32-2), SLB 9672XU20 (Package PG-UQFN-32-1 or PG-UQFN-32-2); Firmware Version: 15.20.15686, 15.21.16430 and 15.22.16832
4348	10/24/2022	Windows Resume	Microsoft Corporation	Software Version: 10.0.18362[1], 10.0.18363[2] and 10.0.19041[3]
4349	10/27/2022	Spectro Cloud Cryptographic Module	Spectro Cloud, Inc.	Software Version: ae223d6138807a13006342edfeef32e813246b39
4350	10/31/2022	Black Lantern(R) Cryptographic Module	Guardtime Federal	Hardware Version: BL400; Firmware Version: BLKSI.2.2.1-FIPS