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

March 2023

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: 2023.04.20 11:04:01 -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 Location: Date: 2023.04.19 17:29:08-04'00' Foxit PDF Editor Version: 12.1.0

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
4446	03/07/2023	SLS37CSAUS V2X	Infineon Technologies AG	Hardware Version: Infineon SLS37CSAUS V2X security controller SLI37CMA2M0-G11; Firmware Version: 01.03.4091
4447	03/09/2023	SonicWALL SMA Series v12.4 SMA 8200v	SonicWall, Inc.	Software Version: v12.4.1-02451; Hardware Version: Intel Xeon Silver 4208
4448	03/13/2023	IPsec IP Gateway Server	Hughes Network Systems, LLC	Hardware Version: 1507355-8022; Firmware Version: IPsec IPGW Firmware Version: 7.4.1.15, Management Gateway Client Firmware Version: 7.4.1.8
4449	03/14/2023	Wavence Microwave radio cryptoModule	Nokia XHAUL	Hardware Version: 1.0, P/N 3DB19060AA, 3DB19060BA, 3DB19060CA, 3DB19060DA, 3DB19060EA, 3DB19060FA, 3DB19060GA, 3DB19060HA, 3DB76047AA, 3DB76047BA, 3DB76047CA, 3DB76047DA, 3DB76047EA, 3DB76047FA, 3DB76047GA, 3DB76047HA, 3DB76048AA, 3DB76048BA, 3DB76048CA, 3DB76048DA, 3DB76049AA, 3DB76049BA, 3DB76049CA, 3DB76049DA, 3DB76050AA, 3DB76050BA, 3DB76050CB, 3DB76050DB, 3DB76050GA, 3DB76050HA, 3DB76078AA, 3DB76078BA, 3DB76123AA, 3DB76123BA; Tamper Evident Seals: P/N 3DB76375AA; Sub-Rack: P/N 3EM22618AC; Sub-Rack Blank Filler Panel: P/N 3EM22616AA; Sub-Rack MA Cover: P/N 3DB76330AA; Firmware Version: BOMPT: V05.04.00; SWMPT: V25.02.41; FARPH: V06.05.07; FM620: V01.06.64; C2620: V00.09.00; P2H24: V00.04.05; FLPAR: V01.00.12; HASH0: V01.00.00
4450	03/14/2023	MPU5	Persistent Systems, LLC	Hardware Version: P/N WR-5100, Versions: 4.0.B, 4.1.B, 4.2.B, 4.2.C, 4.3.B, 4.3.C, 4.3.D, 4.4.B, 4.4.C, 4.4.D, 4.5.C, 4.5.D, 4.6.D, 4.6.K, 4.6.L, 4.6.L.1, 4.6.M, 4.6.N, 4.9.N, 4.9.O and 4.9.P; Tamper Evident Paint P/N PROD-007; Firmware Version: 19.6.10
4451	03/15/2023	Symantec Integrated Secure Gateway	Symantec, A Division of Broadcom	Hardware Version: SSP-S410-10 (090-20000-02)[1], SSP-S410-20 (090-20001-02)[1], SSP-S410-30 (090-20002-02)[1], SSP-S410-40 (090-20003-02)[1] and SSP-S210-10 (090-20012-01)[2] with FIPS KIT HW-KIT-FIPS-S410[1] and HW-KIT-FIPS-S210[2].; Firmware Version: 2.4.2.1
4452	03/15/2023	Symantec Management Center Virtual Appliance	Symantec, A Division of Broadcom	Software Version: 3.3.1.1
4453	03/22/2023	SonicWALL SMA Series v12.4 SMA 6210, SMA 7210, SMA 7200	SonicWall, Inc.	Hardware Version: SMA 6210 [P/N 101-500564-50], SMA 7200 [P/N 101-500398-61 Rev B] and SMA 7210 [P/N 101-500563-50]; Firmware Version: 12.4.1-02451
4454	03/22/2023	TRANSEC Module	iDirect Government, LLC	Hardware Version: E0002268; Firmware Version: Cloak 1.0.3.0
4455	03/22/2023	MFP Cryptographic Module(A)	KYOCERA Document Solutions Inc.	Hardware Version: VaultIP-2.1.10 and EIP38-3.2; Firmware Version: 2.2.18
4456	03/22/2023	Symantec Content Analysis Virtual Appliance	Symantec, A Division of Broadcom	Software Version: 3.1.3.0
4457	03/22/2023	TCB Launcher	Microsoft Corporation	Software Version: 10.0.18363[1] and 10.0.19041[2]; Hardware Version: Intel Core i5-8365U[2] and Intel Core i7-8665U[1]

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4458	03/24/2023	Red Hat Enterprise Linux 8 NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20210708
4459	03/24/2023	VaultIP	Rambus Inc.	Hardware Version: 3.0.3; Firmware Version: 3.0.6
4460	03/28/2023	Apple corecrypto User Space Module for Intel (ccv10)	Apple Inc.	Software Version: 10.0
4461	03/29/2023	Cisco Catalyst 8300 Series Edge Platforms	Cisco Systems, Inc.	Hardware Version: C8300-1N1S-6T, C8300-1N1S-4T2X, C8300-2N2S-6T, and C8300-2N2S-4T2X with component C-NIM-1X; Firmware Version: IOS-XE 17.3
4462	03/29/2023	Acme Packet 4600 and Acme Packet 6350 (v9.0)	Oracle Communications	Hardware Version: 4600 and 6350 with Quad NIU; Firmware Version: S-Cz9.0