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

November 2019

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: Michael Cooper

Dated: 12/2/2019

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: December 2, 2019

Manager, Product Assurance and Standards
Canadian Centre for Cyber Security

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3534	11/02/2019	Cisco Systems Libreswan Cryptographic Module	Cisco Systems, Inc.	Software Version: 3.20
3535	11/07/2019	Cisco Systems Kernel Crypto API Cryptographic Module	Cisco Systems, Inc.	Software Version: 3.10
3559	11/01/2019	Qualcomm(R) Trusted Execution Environment Software Cryptographic Library	Qualcomm Technologies, Inc.	Software Version: 5.2.2-00027; Hardware Version: Snapdragon 855
3560	11/05/2019	SBC 5400 Session Border Controller	Sonus Networks, Inc.	Hardware Version: SBC 5400; Firmware Version: R6.2.2
3561	11/12/2019	Cisco Aironet 1572 EAC, 1702i, 2702e/i, 3702e/i/p Wireless LAN Access Points	Cisco Systems, Inc.	Hardware Version: 1572 EAC, 1702i, 2702e, 2702i, 3702e, 3702i and 3702p with Marvell 88W8764C with FIPS Kit: AIRLAP-FIPSKIT= VERSION A1; Firmware Version: 8.5
3562	11/14/2019	Amazon Linux 2 OpenSSH Server Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
3563	11/15/2019	Red Hat Enterprise Linux Libreswan Cryptographic Module	Red Hat(R), Inc.	Software Version: 7.0
3564	11/15/2019	ProtectServer Internal Express 2 (PSI-E2)	Gemalto	Hardware Version: VBD-05, Version Code 0200; Firmware Version: 5.03.01 and 5.03.02
3565	11/15/2019	Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module	Red Hat(R), Inc.	Software Version: 7.0
3566	11/18/2019	Lenel OnGuard Access Control Cryptographic Module	UTC Fire & Security Americas Corporation, Inc.	Software Version: 7.4.457.69 with Critical On-Demand Hot Fix for DE40714 or 7.5.375.1
3567	11/20/2019	Amazon Linux 2 OpenSSH Client Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
3568	11/21/2019	Hillrom Cryptographic Security Module	Hill-Rom Holdings, Inc.	Software Version: 2.0.10
3569	11/21/2019	Quantum Xchange FIPS Object Module	Quantum Xchange	Software Version: 1.0
3570	11/22/2019	Cisco NCS 5500 Series Routers	Cisco Systems, Inc.	Hardware Version: NCS-5501, NCS-5502, NCS-55A1-36H-SE-S and [NCS-5508 with components NC55-RP, NC55-36X100G-S]; Firmware Version: Cisco IOS XR 6.3
3571	11/25/2019	Red Hat Enterprise Linux GnuTLS Cryptographic Module	Red Hat(R), Inc.	Software Version: 7.0
3572	11/25/2019	FortiGate-51E [1], FortiGate-61E [2], FortiWifi-61E [3], FortiWifi-90D [4] and FortiGateRugged-60D [5]	Fortinet, Inc.	Hardware Version: C1AD19 [1], C1AE14 [2], C1AE18 [3], C1AA12 [4], and C1AB57 [5], with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: FortiOS 5.4, b9791, 170802 [1,4,5] and FortiOS 5.4, b3141, 170602 [2,3]

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3573	11/25/2019	XP8 Encryption Backend SAS I/O Module	Hewlett PackardR, Enterprise	Hardware Version: P/N: 3292522-A(BS12GE) Version: D/D10 or D/D11; Firmware Version: 03.09.34.00