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

July 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: 2023.08.04 16:03:45 -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: 2023.08.01 17:30:09-04'00'
Foxit PDF Editor Version: 12.1.2

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
4547	07/09/2023	Silver Peak EdgeConnect	Silver Peak Systems, Inc.	Firmware Version: ECOS 8.1.9 and ECOS 9.1.0
4548	07/10/2023	Amazon Linux 2 OpenSSL Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
4549	07/11/2023	Cisco Catalyst Embedded Wireless Controller on C9100 Series Access Points	Cisco Systems, Inc.	Hardware Version: 9115AXI with one FIPS Kit: AIR-AP-FIPSKIT=, 9115AXE with one FIPS Kit: AIR-AP-FIPSKIT=, 9120AXI with one FIPS Kit: AIR-AP-FIPSKIT=, 9120AXE with one FIPS Kit: AIR-AP-FIPSKIT=, 9120AXP with one FIPS Kit: AIR-AP-FIPSKIT=, 9130AXI with one FIPS Kit: AIR-AP-FIPSKIT=, 9130AXE with one FIPS Kit: AIR-AP-FIPSKIT=;; Firmware Version: IOS-XE 17.3
4550	07/12/2023	Symantec Messaging Gateway Cryptographic Module	Broadcom	Software Version: 2.2.1
4551	07/17/2023	SecureData Engine	SecureAge Technology	Software Version: 8.0.5
4552	07/19/2023	Nokia 1830 Photonic Service Switch (PSS)	Nokia Corporation	Hardware Version: Chassis (WOMPU00CRA / 3KC48901AA) [1], Chassis (WOMR300BRA / 3KC48960AC) [2] and Chassis (WOM4V10GRA / 8DG59319AB) [3]; 8EC2E Card (3KC48910AA) [1] and 32EC2E Card (8DG63583AA) [2, 3]; 11QPEN4 (8DG60996AA) [1-3] and S13X100E (8DG63988AA) [1-3]; Filler Card (8DG59418AA) [1-3]; Security Label Kit (8DG-6509-AAAA) [1-3]; Firmware Version: 1830PSSECE-10.1-2
4553	07/27/2023	IBM 4769-001 Enterprise PKCS#11 HSM Cryptographic Coprocessor Security Module	IBM	Hardware Version: PN 02WN654-N37880 POST0 v9662 MB0 v6096 (Standard Power); PN 02WN652-N37880 POST0 v9662 MB0 v6096 (Low Power); PN 03FM956-H07053 POST0 v8657 MB0 v6381 (Standard Power); PN 03FM953-H07053 POST0 v8657 MB0 v6381 (Low Power); PN 03JJ168-N38177 POST0 v8657 MB0 v6381 (Standard Power); PN 03JJ165-N38177 POST0 v8657 MB0 v6381 (Low Power); Firmware Version: 7.0.46z P1591 M1591 P5625 F0701 and 7.0.74z P3795 M6356 P0630 F0701
4554	07/28/2023	Cisco Catalyst 9800-CL Wireless Controller	Cisco Systems, Inc.	Software Version: IOS-XE 17.3
4555	07/31/2023	AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U)	Advanced Micro Devices (AMD)	Hardware Version: bc0c0140FIPS001; Firmware Version: bc0c0140FIPS001