FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

TM

The Canadian Centre for Cyber Security

August 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

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Digitally signed
by TIMOTHY
HALL
Date: 2023.09.08
12:58:35 -04'00'

Signed on behalf of the Government of Canada

Signature: King, Lyall

Dated:

Digitally signed by King, Lyall
DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall"
Reason: I am approving this document
Location:
Date: 2023.09.04 15:23:52-04'00'
Foxit PDF Editor Version: 12.1.2

Director, Risk Mitigation Programs
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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4556	08/02/2023	Cisco Catalyst 9200 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst C9200-24T, Cisco Catalyst C9200-48T, Cisco Catalyst C9200-24P, Cisco Catalyst C9200-48P, Cisco Catalyst C9200-24P8X and Cisco Catalyst C9200-48P8X with components C9200-NM-4G, C9200-NM-4X, C9200-NM-2Y and C9200-NM-2Q; Firmware Version: Cisco IOS-XE 16.12 and Cisco IOS-XE 17.3
4557	08/10/2023	BigFix Cryptographic Module	HCL America, Inc.	Software Version: 3.0.8
4558	08/18/2023	IBM 4770-001 Enterprise PKCS#11 HSM Cryptographic Coprocessor Security Module	IBM	Hardware Version: PN 03JJ471-H07163 POST0 v9398 MB0 v9005 (Standard Power); PN 03JJ467-H07163 POST0 v9398 MB0 v9005 (Low Power); PN 03JJ829-N38324 POST0 v8840 MB0 v3606 (Standard Power); PN 03JJ825-N38324 POST0 v8840 MB0 v3606 (Low Power); PN 03KY267-H07190 POST0 v8840 MB0 v3606 (Standard Power); PN 03KY267-H07190 POST0 v8840 MB0 v3606 (Low Power); Firmware Version: 8.0.37z P3592 M3592 P4630 F0D0B
4559	08/21/2023	Aruba 2930F Switch Series	Aruba, a Hewlett Packard Enterprise company	Hardware Version: JL253A, JL254A, JL258A, JL263A, JL264A; Firmware Version: WC.16.11
4560	08/23/2023	KoolSpan Cryptographic Module	KoolSpan, Inc	Software Version: 1.0.2
4561	08/28/2023	ExtraHop Cryptographic Module	ExtraHop Networks, Inc.	Software Version: 1.0
4562	08/29/2023	HID Global ActivID Applet Suite v2.7.4 on Gemalto TOPDLv2.1	HID Global and Gemalto	Hardware Version: NXP P60D144P VA (MPH149); Firmware Version: Gemalto TOPDLV2.1 (Filter04) and HID Global ActivID Applet Suite v2.7.4
4563	08/29/2023	IDPrime PIV v3.0 Applet on IDCore 3130 Platform	Gemalto	Hardware Version: SLE78CFX400VPH with packaging options A1977038 and A2410334 and SLE78CLFX400VPH with packaging option A1714221; Firmware Version: IDCore 3130 (Build09C) with Applets [PIV v3.0 (Build08), PIV Admin v3.0 (Build 08), MoC Server (version 1.1)]
4564	08/30/2023	HID Global ActivID Applet Suite v2.7.5 and v2.7.6 on Giesecke & Devrient Sm@rtCafé Expert 7.0	HID Global and Giesecke+Devrient Mobile Security America Inc.	Hardware Version: SLE78CLFX4000P(M) M7892; Firmware Version: Sm@rtCafé Expert 7.0 and HID Global ActivID Applet Suite 2.7.5 and 2.7.6
4565	08/30/2023	Amazon Linux 2 NSS Cryptographic Module	Amazon Web Services, Inc.	Software Version: 1.0
4566	08/30/2023	Juniper CryptoCore Cryptographic Module	Juniper Networks, Inc.	Software Version: 1.0
4567	08/30/2023	Ruckus Networks Virtual SmartZone - Data Plane (vSZ-D)	CommScope Technologies LLC	Software Version: 5.2.1.3
4568	08/30/2023	Ruckus Networks Virtual SmartZone (vSZ)	CommScope Technologies LLC	Software Version: 5.2.1.3
4569	08/30/2023	Ruckus Networks SmartZone 144 (SZ-144) and SmartZone 300 (SZ-300) WLAN Controllers	CommScope Technologies LLC	Hardware Version: PF1-S144-US00, RevA; PF1-S300-WW00, RevA; PF1-S300-WW10, RevA; Firmware Version: 5.2.1.3

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
4570	08/30/2023	Apple corecrypto User Space Module for ARM (ccv10)	Apple Inc.	Software Version: 10.0
4571	08/31/2023	Aruba 2930M, 3810M and 5400R zl2 Switch Series	Aruba, a Hewlett Packard Enterprise company	Hardware Version: Aruba 2930M Switches (JL319A, JL320A, JL321A, JL322A, JL323A, and JL324A) [1] with Expansion Cards listed in Table 2 of the Security Policy, Aruba 3810M Switches (JL071A, JL072A, JL073A, JL074A, JL075A, and JL076A) [2] with Expansion Cards listed in Table 3 of the Security Policy, Aruba 5400R zl2 Switches (5406R zl2 J9821A and 5412R zl2 J9822A) [3] with Management card and Interface Cards listed in Table 4 of the Security Policy; Firmware Version: WC.16.11 [1] and KB.16.11 [2] or [3]
4572	08/31/2023	Aruba 2930F, 2930M, 3810M and 5400R zl2 Switch Series	Aruba, a Hewlett Packard Enterprise company	Hardware Version: Aruba 2930F Switches (JL258A, JL259A, JL260A, JL261A, JL262A, JL263A, JL264A, JL557A, JL559A and JL692A) [1], Aruba 2930M Switches (JL319A, JL320A, JL321A, JL322A, JL323A, JL324A, R0M67A and R0M68A) [1] with Expansion Cards listed in Table 3 of the Security Policy, Aruba 3810M Switches (JL071A, JL072A, JL073A, JL074A, JL075A and JL076A) [2] with Expansion Cards listed in Table 4 of the Security Policy, Aruba 5400R zl2 Switches (5406R zl2 J9821A and 5412R zl2 J9822A) [2] with Management card and Interface Cards listed in Table 5 of the Security Policy; Firmware Version: WC.16.11 [1] or KB.16.11 [2]
4573	08/31/2023	LifeCare PCA™ Infusion Pump	ICU Medical, Inc.	Hardware Version: P/Ns 20837-04-07 and 20837-04-08 with components 810-04505-039 and 810-11438-018; Firmware Version: CE v1.90.1.4 and MCU v7.4.1.3
4574	08/31/2023	Titan Security Key, Chip Boundary	Google, LLC.	Hardware Version: H1B2; Firmware Version: 1.2
4575	08/31/2023	Security Builder FIPS Java Module	BlackBerry Certicom	Software Version: 2.9[1], 2.9.2[2]
4576	08/31/2023	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.2
4577	08/31/2023	Samsung SCrypto Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: 2.4