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 2021

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: Gavin O'Brien

Dated: 04/01/2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 04/01/2021

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
3831	03/01/2021	GigaVUE-HC2 Visibility Appliance	Gigamon Inc.	Hardware Version: GVS-HC201 and GVS-HC202 (Chassis) with SMT-HC0-Q02X08 Gen2 (GigaSMART), SMT-HC0-R (GigaSMART) and CTL-HC0-002 (Controller); FIPS Tamper Label SKU: ACC-HC0-FIPS; Firmware Version: 5.9.00.05
3832	03/02/2021	GigaVUE-HC3 Visibility Appliance	Gigamon Inc.	Hardware Version: GVS-HC3A1 and GVS-HC3A2 (Chassis) with SMT-HC3-C05 (GigaSMART) and CTL-HC3-002 (Controller) and GVS-HC3-EXT; FIPS Tamper Label SKU: ACC-HC0-FIPS; Firmware Version: 5.9.00.05
3833	03/03/2021	FortiGate-1101E/2000E/2201E/2500E/3301E	Fortinet, Inc.	Hardware Version: FortiGate-1101E (C1AJ13) [1], FortiGate-2201E (C1AH54) [2], FortiGate-3301E (C1AJ38) [2], FortiGate-2000E (C1AF49) [3] and FortiGate-2500E (C1AF51) [3] with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 6.0 build 5441 and FortiOS 6.2 build 5525 [1], FortiOS 6.0 build 5440 and FortiOS 6.2 build 5611 [2], FortiOS 6.0 build 5445 and FortiOS 6.2 build 5548 [3]
3834	03/03/2021	Cisco Catalyst 9400 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9404R, Cisco Catalyst C9407R and Cisco Catalyst C9410R with components C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-LC-48U, C9400-LC-48T, C9400-LC-48P, C9400-LC-24XS, C9400-LC-48UX, C9400-LC-24S, C9400-LC-48S and C9400-LC-48H; Firmware Version: Cisco IOS-XE 16.12
3835	03/03/2021	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
3836	03/03/2021	Rancher Kubernetes Cryptographic Library	Rancher Labs	Software Version: 66005f41fbc3529ffe8d007708756720529da20d
3837	03/03/2021	ESCRYPT's CycurLIB	Landis+Gyr	Software Version: 3.5.3-FIPS-1.2
3838	03/04/2021	Cryptographic Module for Intel® Platforms' Security Engine Chipset	Intel Corporation	Hardware Version: 3.1; Firmware Version: 3.0
3839	03/04/2021	Red Hat Enterprise Linux 8 NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20190808
3840	03/05/2021	SE050	NXP Semiconductors	Hardware Version: [SE050 (N7121 B1)]; Firmware Version: [Platform ID 4A335233353130323634353731313030034D67740BE14219 and ROM ID 2E5AD88409C9BADB and Patch ID 1 and SE050 IoT applet v3.6.0]
3841	03/08/2021	F5(R) Device Cryptographic Module	F5 Networks, Inc	Hardware Version: BIG-IP i7800 and BIG-IP 10350v-F with FIPS Kit P/N: F5-ADD-BIG-FIPS140; Firmware Version: 14.1.2
3842	03/08/2021	Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel8.20200305.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3843	03/10/2021	Cisco Adaptive Security Appliance (ASA) Virtual	Cisco Systems, Inc.	Software Version: 9.12
3844	03/12/2021	Juniper Networks MX10003 3D Universal Edge Router with JNP-MIC1-MACSEC MACSec MIC and EX9253 Ethernet Switch with EX9253-6Q12C-M MACSec Line Card	Juniper Networks, Inc.	Hardware Version: MX10003 and EX9253 with components identified in Security Policy Table 1; Firmware Version: Junos OS 19.3R1
3846	03/13/2021	VMware's BoringCrypto Module	VMware, Inc.	Software Version: 1.0
3848	03/15/2021	SUSE Linux Enterprise Server libgcrypt Cryptographic Module	SUSE, LLC	Software Version: 3.0
3849	03/15/2021	RX65N-2MB Security Management Module	Renesas Electronics Corporation	Hardware Version: R5F565NEHDFC; Firmware Version: Secure Boot: Ver.1.00, Crypto Firmware: Ver.1.00
3850	03/18/2021	DocuSign Signature Appliance	DocuSign, Inc.	Hardware Version: 8.0; Firmware Version: 9.3.9.20
3851	03/18/2021	Titan Security Key, Chip Boundary	Google, LLC.	Hardware Version: H1B2; Firmware Version: 1.2
3852	03/18/2021	Cisco Catalyst 9200L Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst C9200L-24P-4G, Cisco Catalyst C9200L-24P-4X, Cisco Catalyst C9200L-24T-4G, Cisco Catalyst C9200L-24T-4X, Cisco Catalyst C9200L-48P-4G, Cisco Catalyst C9200L-48P-4X, Cisco Catalyst C9200L-48T-4G, Cisco Catalyst C9200L-48T-4X, Cisco Catalyst C9200L-24P8X-2Y, Cisco Catalyst C9200L-24P8X-4X, Cisco Catalyst C9200L-48P12X-4X and Cisco Catalyst C9200L-48P8X-2Y; Firmware Version: Cisco IOS-XE 16.12
3853	03/18/2021	Cisco Catalyst 9300 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9300-24S, Cisco Catalyst 9300-48S,Cisco Catalyst 9300L-24T-4G, Cisco Catalyst 9300L-24P-4G, Cisco Catalyst 9300L-48T-4G, Cisco Catalyst 9300L-48P-4G, Cisco Catalyst 9300L-24T-4X, Cisco Catalyst 9300L-24P-4X, Cisco Catalyst 9300L-48T-4X, Cisco Catalyst 9300L-48P-4X, Cisco Catalyst 9300L-24UX-4X, Cisco Catalyst 9300L-48UX-4X, Cisco Catalyst 9300L-24UX-2Q and Cisco Catalyst 9300L-48UX-2Q; Firmware Version: Cisco IOS-XE 16.12
3854	03/18/2021	HID Global Applets v3.0 on NXP JCOP 3 SecID P60 CS (OSB)	HID Global	Hardware Version: P6022y VB with product identifier J3H145C; Firmware Version: 19790400 and HID Global ActivID Applet Suite v3.0 with factory configuration FIPS 140-2-L2
3855	03/23/2021	Apple corecrypto Kernel Space Module for ARM (ccv10)	Apple Inc.	Software Version: 10.0
3856	03/23/2021	Apple corecrypto User Space Module for ARM (ccv10)	Apple Inc.	Software Version: 10.0

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3857	03/24/2021	VMware's OpenSSL FIPS Object Module	VMware, Inc.	Software Version: 2.0.20-vmw
3858	03/24/2021	Apple corecrypto Kernel Space Module for Intel (ccv10)	Apple Inc.	Software Version: 10.0
3859	03/24/2021	Apple corecrypto User Space Module for Intel (ccv10)	Apple Inc.	Software Version: 10.0
3860	03/24/2021	Red Hat Enterprise Linux 7 NSS Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190606
3861	03/24/2021	Motorola Solutions Cryptographic Firmware Module	Motorola Solutions, Inc.	Firmware Version: R01.03.00
3862	03/24/2021	Motorola Solutions Cryptographic Firmware Module	Motorola Solutions, Inc.	Firmware Version: R01.07.00
3863	03/24/2021	ID-One PIV 2.4 on Cosmo V8.2 NPIVP & CIV Configurations	IDEMIA	Hardware Version: P/N '30'; Firmware Version: ['6F01' with ID-One PIV Applet 2.4.2 NPIVP configuration] and ['6F01' with ID-One PIV Applet 2.4.2 CIV configuration]
3864	03/24/2021	ID-One PIV 2.4 on Cosmo V8.2 SPE Configurations	IDEMIA	Hardware Version: P/N '30'; Firmware Version: ['6F01' with ID-One PIV Applet 2.4.2 SPE configuration] and ['6F01' with ID-One PIV Applet 2.4.2 SPE-EP configuration]
3865	03/25/2021	Vocera Smartbadge Cryptographic Module	Vocera Communications, Inc.	Firmware Version: 5.0
3866	03/25/2021	Zebra BoringSSL Cryptographic Module	Zebra Technologies Corporation	Software Version: 1.0
3867	03/29/2021	Red Hat Enterprise Linux 7 OpenSSL Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190409
3868	03/29/2021	Cisco Catalyst 9600 Series Switches	Cisco Systems, Inc.	Hardware Version: Cisco Catalyst 9606R with components C9600-SUP-1, C9600-LC-48YL and C9600-LC-24C; Firmware Version: Cisco IOS-XE 16.12
3869	03/29/2021	Network Security Platform Sensor NS7100, NS7200 and NS7300	McAfee, LLC	Hardware Version: P/Ns IPS-NS7100 Version 1.00, IPS-NS7200 Version 1.00 and IPS-NS7300 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.1
3870	03/29/2021	Network Security Platform Sensor NS7150, NS7250 and NS7350	McAfee, LLC	Hardware Version: P/Ns IPS-NS7150 Version 1.00, IPS-NS7250 Version 1.00 and IPS-NS7350 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.1
3871	03/29/2021	Network Security Platform Sensor NS9100 and NS9200	McAfee, LLC	Hardware Version: P/Ns IPS-NS9100 Version 1.00 and IPS-NS9200 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.1
3872	03/29/2021	Network Security Platform Sensor NS9300 S	McAfee, LLC	Hardware Version: P/Ns IPS-NS9300 S Version 1.30; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.1

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

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3873	03/29/2021	Network Security Platform Sensor NS9300P	McAfee, LLC	Hardware Version: P/Ns IPS-NS9300 P Version 1.30; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.1
3874	03/29/2021	Cisco Catalyst 9800-CL Wireless Controller	Cisco Systems, Inc.	Software Version: IOS-XE 16.12
3875	03/29/2021	VMware OpenSSL FIPS Object Module	VMware, Inc.	Software Version: 2.0.9
3876	03/30/2021	CryptoComply for HSM	SafeLogic Inc.	Hardware Version: NC4035E-000 and NC4335N-000, Build Standard A; Firmware Version: 12.50.11
3877	03/30/2021	Cisco Firepower 2100 Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR2110-NGFW-K9, FPR2120-NGFW-K9, FPR2130-NGFW-K9, FPR2140-NGFW-K9 with FIPS Kit (AIR-AP-FIPSKIT=) and opacity shield 69-100250-01; Firmware Version: 9.12
3878	03/30/2021	Network Security Platform Sensor NS3100, NS3200, NS5100 and NS5200	McAfee, LLC	Hardware Version: P/Ns IPS-NS3100 Version 1.00, IPS-NS3200 Version 1.00, IPS-NS5100 Version 1.00 and IPS-NS5200 Version 1.00; FIPS Kit P/N IAC-FIPS-KT2; Firmware Version: 10.1.17.1