

FIPS 140-2 Consolidated Validation Certificate



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



February 2018



The Communications Security Establishment of the Government of Canada

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, 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 J. Cooper
Dated: 3/5/2018
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature: [Signature]
Dated: 03/05/2018
Director, Architecture and Technology Assurance
Communications Security Establishment

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
3116	02/02/2018	Voice Processing Module Cryptographic Module (VPMCM) / Telephone Media Gateway Cryptographic Module (TMGCM)	Motorola Solutions, Inc.	Hardware Version: P/Ns VPMCRYPTO_B or VPMCRYPTO_C; Firmware Version: R01.11.00
3117	02/06/2018	Brocade® X6-8 and X6-4 Directors	Brocade Communications Systems, Inc.	Hardware Version: {BR-X64-001 (80-1009190-01) with FRUs (80-1009332-01, 80-1009341-01, 80-1009225-01, 80-1009227-01, 80-1009326-01, 80-1009441-01, 80-1009349-01, 80-1009348-01, 80-1009348-01), BR-X68-001 (80-1009230-01) with FRUs (80-1009332-01, 80-1009342-01, 80-1009225-01, 80-1009227-01, 80-1009326-01, 80-1009441-01, 80-1009349-01, 80-1009348-01, 80-1009348-01)} with FIPS Kit Brocade XBR-000195 (P/N: 80-1002006-02); Firmware Version: Fabric OS v8.1.0 (P/N 63-1001736-01)
3118	02/07/2018	iRhythm Cryptographic Module	iRhythm Technologies, Inc.	Software Version: 2.1
3119	02/07/2018	FireEye CM Series: CM-4500, CM-7500, CM-9500	FireEye, Inc.	Hardware Version: CM-4500, CM-7500, CM-9500; Firmware Version: 8.0
3120	02/07/2018	FireEye EX Series: EX-3500, EX-5500, EX-8500	FireEye, Inc.	Hardware Version: EX-3500, EX-5500, EX-8500; Firmware Version: 8.0
3121	02/07/2018	FireEye VX Series: VX-5500, VX-12500	FireEye, Inc.	Hardware Version: VX-5500, VX-12500; Firmware Version: 8.0
3122	02/08/2018	iLO 5 Cryptographic Module	Hewlett Packard Enterprise Development LP	Hardware Version: ASIC (GXP: 815393-001) with Flash Memory (1819-1208), NVRAM (1819-1209), and DDR3 SDRAM (2660-0461); Firmware Version: 1.11
3123	02/09/2018	QTI Crypto Engine Core	Qualcomm Technologies, Inc.	Hardware Version: 5.4.1
3124	02/09/2018	QTI Inline Crypto Engine (UFS)	Qualcomm Technologies, Inc.	Hardware Version: 3.1.0
3125	02/12/2018	Trend Micro Cryptographic Module	Trend Micro, Inc.	Software Version: 1.0
3126	02/13/2018	Splunk Cryptographic Module	Splunk Inc.	Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16
3127	02/14/2018	FireEye CMS Series: CM2500V, CM7500V	FireEye, Inc.	Software Version: 8.0
3128	02/14/2018	Brocade® G620 FC Switch	Brocade Communications Systems, Inc.	Hardware Version: {BR-G620-48-32G-F Switch (P/N 80-1009066-02) with FRU (P/N 80-1009260-01) and POD License (P/N 80-1009038-01), BR-G620-48-32G-R Switch (P/N 80-1009067-02) with FRU (P/N 80-1009261-01) and POD License (P/N 80-1009038-01)} with FIPS Kit Brocade XBR-000195 (P/N 80-1002006-02); Firmware Version: Fabric OS v8.1.0 (P/N 63-1001736-01)
3129	02/15/2018	Trend Micro Mobile Cryptographic Module	Trend Micro, Inc.	Software Version: 1.0
3130	02/15/2018	EnterpriseDB Cryptographic Module	EnterpriseDB	Software Version: 2.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3132	02/20/2018	FireEye NX Series: NX1500V, NX2500V, NX2550V, NX4500V, NX6500V	FireEye, Inc.	Software Version: 8.0
3133	02/21/2018	PA-200, PA-220, PA-500, PA-800 Series, PA-3000 Series, PA-5000 Series, PA-5200 Series and PA-7000 Series Firewalls	Palo Alto Networks	Hardware Version: PA-200 P/N 910-000015 Rev. E with [1], PA-220 P/N 910-000128 Rev. A with [1], PA-500 P/N 910-000006 Rev. O with [2], PA-500-2GB P/N 910-000094 Rev. O with [2], PA-820 P/N 910-000120 Rev. A with [3], PA-850 P/N 910-000119 Rev. A with [3], PA-3020 P/N 910-000017 Rev. J with [4], PA-3050 P/N 910-000016 Rev. J with [4], PA-3060 P/N 910-000104 Rev. C with [5], PA-5020 P/N 910-000010 Rev. F with [6], PA-5050 P/N 910-000009 Rev. F with [6], PA-5060 P/N 910-000008 Rev. F with [6], PA-5220 P/N 910-000132 Rev. A with [7], PA-5250 P/N 910-000131 Rev. A with [7], PA-5260 P/N 910-000125 Rev. A with [7], PA-7050 P/N 910-000102 Rev. B with [8] and at least one from [10] and PA-7080 P/N 910-000122 Rev. A with [9] and at least one from [10]; FIPS Kit: P/Ns 920-000084 Rev. A [1], 920-000005 Rev. A [2], 920-000185 Rev. A [3], 920-000081 Rev. A [4], 920-000138 Rev. A [5], 920-000037 Rev. A [6], 920-000186 Rev. A [7], 920-000112 Rev. A [8] and 920-000119 Rev. A [9]; Network Processing Cards [10]: P/Ns 910-000028-00B, 910-000117-00A, 910-000137-00A and 910-000136-00A; Firmware Version: 8.0.3
3134	02/21/2018	Seagate Secure(R) TCG Opal SSC Self-Encrypting Drive	Seagate Technology LLC	Software Version: N/A; Hardware Version: 9WU142 [1, 2, 3, 4, 5], 9WU14C [1, 2, 3, 4, 5], 9WU141 [1, 2, 3, 4, 5], 1DJ142 [1, 5, 6, 7], 1DJ14C [1, 5, 6, 7], 1DJ141 [1, 5, 6, 7], 1RS152 [1, 8, 9, 10], 1RS15C [1, 8, 9, 10] and 1RS15D [1, 8, 9, 10]; Firmware Version: 0001SDM7 [1], 0001SED7 [2], 0002SDM7 [3], 0002SED7 [4], 0001LIM7 [5], 1002SED7 [6], 1003SED7 [7], 0001YXM7 [8], 0002LIM7 [9] or 0004LIM7 [10]
3135	02/22/2018	Brocade® 7840 Extension Switch	Brocade Communications Systems, Inc.	Hardware Version: {7840 Extension Switch (P/N 80-1008000-01) with FRUs (80-1004580-02 and 80-1007263-01)} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v8.1.0 (P/N 63-1001736-01)
3136	02/23/2018	Juniper Networks SRX1500, SRX4100 and SRX4200 Services Gateways	Juniper Networks, Inc.	Hardware Version: SRX1500 SYS-JB-AC, SRX1500 SYS-JB-DC, SRX4100 SYS-JB-AC, SRX4100 SYS-JB-DC, SRX4200 SYS-JB-AC, SRX4200 SYS-JB-DC; with Tamper Seals JNPR-FIPS-TAMPER-LBLS; Firmware Version: JUNOS 15.1X49-D100
3137	02/26/2018	Juniper Networks vSRX Virtual Firewall	Juniper Networks, Inc.	Software Version: JUNOS 15.1X49 - D100
3138	02/26/2018	OneView Java Crypto Module	Hewlett Packard Enterprise	Software Version: 1.0
3139	02/26/2018	AWS Key Management Service HSM	Amazon Web Services, Inc.	Hardware Version: 2.0; Firmware Version: 1.4.3
3140	02/26/2018	Trend Micro Java Crypto Module	Trend Micro Inc.	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3141	02/27/2018	DocuSign Signature Appliance	DocuSign, Inc.	Hardware Version: 8.0; Firmware Version: 8.5
3142	02/28/2018	F5® Device Cryptographic Module	F5 Networks	Hardware Version: BIG-IP i4000, BIG-IP i5000, BIG-IP i7000, BIG-IP 4000, BIG-IP 7000, BIG-IP 10350F, VIPRION B2250, VIPRION B4450; Firmware Version: 13.1.0