FIPS 140-2 Consolidated Validation Certificate

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

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0035

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, 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: 1/9/14

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 2 January 2014.

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

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
2009	11/05/2013	Wi-Q Communication Server Cryptographic Module	Stanley Security Solutions, Inc.	Software Version: 3.0.27
2010	11/05/2013	FortiGate-5140 Chassis with FortiGate 5000 Series Blades	Fortinet, Inc.	Hardware Version: Chassis: C4GL51; Blades: P4CF76, P4CJ36-02, P4CJ36-04 and P4EV74; AMC Components: P4FC12 and AMC4F9; Shelf Manager: PN 21594 346; Alarm Panel: PN 21594 159; Air Filter: PN P10938-01; Front Filler Panel: PN P10945-01: ten; Rear Filler Panel: PN P10946-01: fourteen; Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 4.0, build3767, 130920
2011	11/05/2013	FortiGate-200B [1], FortiGate-300C [2], FortiGate-310B [3], FortiGate-600C [4] and FortiGate-620B [5]	Fortinet, Inc.	Hardware Version: C4CD24 [1], C4HY50 [2], C4ZF35 [3], C4HR40 [4] and C4AK26 [5] with Tamper Evident Seal Kits: FIPS-SEAL-BLUE [1, 3, 5] or FIPS-SEAL-RED [2,4]; Firmware Version: FortiOS 4.0, build3767, 130807
2012	11/05/2013	Juniper Networks Pulse Cryptographic Module	Juniper Networks, Inc.	Software Version: 1.0
2013	11/05/2013	DSI V2VNet Mobile Crypto Module	Dispersive Solutions, Inc.	Software Version: 1.0
2014	11/05/2013	Atmel Trusted Platform Module	Atmel Corporation	Hardware Version: AT97SC3204-X4A1, AT97SC3204-X4A and AT97SC3204-X4M; Firmware Version: 1.2.29.01
2015	11/07/2013	Apple OS X CoreCrypto Module, v4.0	Apple Inc.	Software Version: 4.0
2016	11/07/2013	Apple OS X CoreCrypto Kernel Module, v4.0	Apple Inc.	Software Version: 4.0
2017	11/07/2013	AP 71xx Series Wireless Access Points - AP 7131N, AP 7131N-GR, AP 7161, AP 7181	Motorola Solutions, Inc.	Hardware Versions: AP7131N, AP7131N-GR, AP7161, AP7181; Firmware Version: 5.4.10.0-050GR

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2018	11/07/2013	Imation S250/D250	Imation Corp.	Hardware Versions: D2-S250-S01, D2-S250-S02, D2-S250-S04, D2-S250-S08, D2-S250-S16, D2-S250-S32, D2-D250-B01, D2-D250-B02, D2-D250-B04, D2-D250-B08, D2-D250-B16, D2-D250-B32 and D2-D250-B64; Firmware Version: 4.0.4
2019	11/07/2013	HP LTO-6 Tape Drive	Hewlett-Packard Company	Hardware Versions: AQ278A #912 [1], AQ278B #901 [2], AQ278C #704 [3], AQ288D #103 [4], AQ298C #103 [5], and AQ298A #900 [6]; Firmware Version: J2AW [1], J2AZ [2], J2AS [3], 32AW [4], 22CW [5], and 22CZ [6]
2020	11/07/2013	Apple iOS CoreCrypto Module, v4.0	Apple Inc.	Hardware Version: A4, A5, A6 and A7; Software Version: 4.0
2021	11/07/2013	Apple iOS CoreCrypto Kernel Module, v4.0	Apple Inc.	Software Version: 4.0
2023	11/08/2013	Nuvoton TPM 1.2	Nuvoton Technology Corporation	Hardware Version: FD5C37; Firmware Version: 4.1.5
2024	11/12/2013	CoCo Cryptographic Module 2.0	Coco Communications	Software Version: 2.0
2025	11/12/2013	Blue Coat Systems, Software Cryptographic Module	Blue Coat Systems, Inc.	Software Version: 1.0
2026	11/12/2013	McAfee Database Security Server Cryptographic Module	McAfee, Inc.	Software Version: 1.0
2029	11/13/2013	Atos Worldline Adyton Cryptographic Module	Atos Worldline	Hardware Version: 9071000001; Firmware Version: 1.2.0
2030	11/13/2013	Aspen	Sony Corporation	Hardware Version: 1.0.0; Firmware Versions: 1.0.0 or 1.0.1
2031	11/13/2013	Stonesoft Cryptographic Library	Stonesoft Corporation	Software Version: 1.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2032	11/13/2013	VDX 6710, VDX 6720, VDX 6730 and VDX 8770 with Network OS (NOS) v3.0.1 Firmware	Brocade Communications Systems, Inc.	Hardware Versions: VDX6710-54-F (P/N 80-1004843-04), VDX6710-54-R (P/N 80-1004702-04), VDX6720-16-F (P/N 80-1004566-07, 80-1006701-02), VDX6720-16-R (P/N 80-1004567-07, 80-1006702-02), VDX6720-24-F (P/N 80-1004564-07, 80-1006699-02), VDX6720-24-R (P/N 80-1004564-07, 80-1006700-02), VDX6720-40-F (P/N 80-1004565-07, 80-1006305-02), VDX6720-40-R (P/N 80-1004571-07, 80-1006306-2), VDX6720-60-F (P/N 80-1004568-07, 80-1006303-02), VDX6720-60-R (P/N 80-1004569-07, 80-1006304-02), VDX6730-16-F (P/N 80-1005469-03, 80-1006709-02), VDX6730-16-R (P/N 80-1005651-03, 80-1006711-02), VDX6730-24-F (P/N 80-1005648-03, 80-1006708-02), VDX6730-24-R (P/N 80-1005650-03, 80-1006710-02), VDX6730-40-F (P/N 80-1005680-03, 80-1006719-02), VDX6730-40-R (P/N 80-1005681-03, 80-1006720-02), VDX6730-60-F (P/N 80-1005679-03, 80-1006718-02), VDX6740-60-R (P/N 80-1005678-03, 80-1006717-02), VDX8770-4 (P/N 80-1005850-02, 80-1006532-02) and VDX8770-8 (P/N 80-1005905-02, 80-1006533-02) with FIPS Kit (P/N Brocade XBR-000195); Firmware Version: Network OS (NOS) v3.0.1
2033	11/13/2013	RSA BSAFE Crypto-J Software Module	RSA, The Security Division of EMC	Software Version: 4.1
2034	11/13/2013	Cisco FIPS Object Module	Cisco Systems, Inc.	Software Versions: 3.0 and 3.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2035	11/13/2013	Brocade ICX 6610 Series Stackable Switch with FastIron 7.3.00c Firmware	Brocade Communications Systems, Inc.	Hardware Versions: ICX 6610-24F-I (P/N: 80-1005350-03), ICX 6610-24F-E (P/N: 80-1005345-03), ICX 6610-24-I (P/N: 80-1005348-04), ICX 6610-24-E (P/N: 80-1005343-04), ICX 6610-24P-I (P/N: 80-1005349-05, ICX 6610-24P-E (P/N: 80-1005344-05), ICX 6610-48-I (P/N: 80-1005351-04, ICX 6610-48-E (P/N: 80-1005346-04, ICX 6610-48P-I (P/N: 80-1005352-05) and ICX 6610-48P-E (P/N: 80-1005347-05); with FIPS kit XBR-0000195; Firmware Version: FastIron (FI) v7.3.00c
2036	11/13/2013	Luna® PCI-E Cryptographic Module	SafeNet, Inc.	Hardware Version: VBD-05, Version Code 0103; Firmware Version: 6.3.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2037	11/13/2013	Brocade DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones; 6510 FC Switch; 6520 FC Switch; and 7800 Extension Switch	Brocade Communications Systems, Inc.	Hardware Versions: {[DCX Backbone P/Ns 80-1001064-10, 80-1006751-01, 80-1004920-04 and 80-1006752-01; DCX 8510-8 Backbone P/Ns 80-1004917-04 and 80-1007025-01; DCX-4S Backbone P/Ns 80-1002071-10, 80-1006773-01, 80-1002066-10 and 80-1006772-01; DCX 8510-4 Backbone P/Ns 80-1004697-04, 80-1006963-01, 80-1005158-04 and 80-1006964-01)] with Blade P/Ns 80-1001070-07, 80-1006794-01, 80-1004897-01, 80-1004898-01, 80-1002000-02, 80-1006771-01, 80-1001071-02, 80-1006750-01 80-1000696-01, 80-1005166-02, 80-1005187-02, 80-1001066-01, 80-1006936-01, 80-1001067-01, 80-1006779-01, 80-1001453-01, 80-1006823-01, 80-1003887-01, 80-1007000-01, 80-1002762-04, 80-1006991-01, 80-1000233-10, 80-1002839-03, 80-1007017-01, 49-1000016-04, 49-1000064-02 and 49-1000294-05; 6510 FC Switch P/Ns 80-1005232-03, 80-1005267-03, 80-1005268-03, 80-1005269-03, 80-1005271-03 and 80-1005272-03; 6520 FC Switch P/Ns 80-1007245-01, 80-1007246-01, 80-1007242-01, 80-1007244-01 and 80-1007257-01; 7800 Extension Switch P/Ns 80-1002607-07, 80-1006977-02, 80-1002608-07, 80-1006980-02, 80-1002609-07 and 80-1006979-02} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v7.1.0 (P/N 63-1001187-01)
2038	11/15/2013	CryptoComply™ | Server	SafeLogic, Inc.	Software Version: 2.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2039	11/15/2013	Datacryptor® Gig Ethernet and 10 Gig Ethernet	Thales e-Security	Hardware Version: 1600x433, Rev. 02 and 1600x437, Rev. 02; Firmware Version: 5.0
2040	11/15/2013	McAfee Firewall Enterprise S1104, S2008, S3008, S4016, S5032 and S6032	McAfee, Inc.	Hardware Versions: (FWE-S1104, FWE-S2008, FWE-S3008, FWE-S4016, FWE-S5032 and FWE-S6032) with FRU-686-0089-00; Firmware Version: 8.3.1
2041	11/15/2013	Datacryptor® Gig Ethernet and 10 Gig Ethernet	Thales e-Security	Hardware Version: 1600x433, Rev. 02 and 1600x437, Rev. 02; Firmware Version: 5.0
2042	11/15/2013	Datacryptor® SONET/SDH OC-3/12/48/192C	Thales e-Security	Hardware Version: 1600x435, Rev. 02 and 1600x427, Rev. 02; Firmware Version: 5.0
2043	11/15/2013	HP LTO-6 Tape Drive	Hewlett-Packard Company	Hardware Version: AQ278A #912 [1], AQ278C #704 [2], AQ288D #103 [3], and AQ298C #103 [4]; Firmware Version: J2AW [1], J2AS [2], 32AW [3], and 22CW [4]
2044	11/18/2013	Samsung Key Management Module	Samsung Electronics Co., Ltd.	Software Versions: KM1.1 and KM1.3
2045	11/18/2013	Mocana Cryptographic Suite B Module	Mocana Corporation	Software Version: 5.5fs
2046	11/18/2013	XTM 515, XTM 525, XTM 535 and XTM 545	WatchGuard Technologies, Inc.	Hardware Versions: NC2AE8 (XTM 515, XTM 525, XTM 535 and XTM 545) with Tamper Evident Seal Kit: SKU WG8566; Firmware Version: Fireware XTM OS v11.5.5
2047	11/25/2013	RSA BSAFE® Crypto-C Micro Edition	RSA, The Security Division of EMC	Hardware Version: SPARC T4; Software Version: 4.0.1
2048	11/27/2013	Allegro Cryptographic Engine	Allegro Software Development Corporation	Software Version: 1.1.8
2049	11/27/2013	SafeNet Software Cryptographic Library	SafeNet, Inc.	Software Version: 1.0