

FIPS 140-2 Consolidated Validation Certificate



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



The Communications Security
Establishment of the Government of
Canada

January 2016

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 Feb 2016

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of the Canada

Signature: DL McEly

Dated: 01 Feb 2016

For Director, Architecture and Technology Assurance
Communications Security Establishment Canada

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2517	01/05/2016	FortiManager-1000D	Fortinet Inc.	Hardware Version: C1AA82-01AA-0000 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: v5.2.4-build0738 150923 (GA)
2518	01/05/2016	FortiManager-4000D	Fortinet Inc.	Hardware Version: C1AA62-01AA-0000 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: v5.2.4-build0738 150923 (GA)
2519	01/05/2016	HP FlexFabric 5900CP and 12910 Switch Series	Hewlett-Packard Company	Hardware Version: HP 12910 and [HP 5900CP with JG719A] with FIPS Kit: JG585A or JG586A; Firmware Version: 7.1.045
2520	01/05/2016	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type B	Toshiba Corporation	Hardware Version: A0 with PX04SVQ080B or PX04SVQ160B; Firmware Version: ZW00
2521	01/05/2016	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type A	Toshiba Corporation	Hardware Version: A0 with PX04SVQ080B or PX04SVQ160B; Firmware Version: ZZ00
2522	01/05/2016	McAfee Web Gateway Virtual Appliance	Intel Corporation	Software Version: 7.3.2.3.4
2523	01/05/2016	McAfee Web Gateway WBG-5000-C and WBG-5500-C Appliances	Intel Corporation	Hardware Version: WBG-5000-C and WBG-5500-C; Firmware Version: 7.3.2.3.4
2524	01/05/2016	HyTrust KeyControl (TM) Cryptographic Module	HyTrust, Inc.	Software Version: 1.0
2525	01/05/2016	CounterTack Sentinel Endpoint Module	CounterTack, Inc.	Software Version: 3.6.6
2526	01/05/2016	FortiAnalyzer 5.2	Fortinet Inc.	Firmware Version: v5.2.4-build0738 150923(GA)
2527	01/05/2016	Postal mRevenector US 2014	Francotyp-Postalia GmbH	Hardware Version: Hardware P/N: 580036020300/01; Firmware Version: Bootloader: 90.0036.0201.00/2011485001; Softwareloader: 90.0036.0206.00/2011485001; US Application: 90.0036.0216.00/2014472001
2528	01/10/2016	FortiAnalyzer-3000D	Fortinet Inc.	Hardware Version: C1AA61-03AA-0000 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: v5.2.4-build0738 150923(GA)
2529	01/11/2016	FortiAnalyzer-200D	Fortinet Inc.	Hardware Version: C4FA20-01AA-0000 with Tamper Evident Seal Kits: FIPS-SEAL-RED; Firmware Version: v5.2.4-build0738 150923 (GA)

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2530	01/11/2016	Brocade(R) FCX 624/648, ICX (TM) 6610, ICX 6450, ICX 7750, ICX 7450 and SX 800/1600 Series	Brocade Communications Systems, Inc.	Hardware Version: {[FCX624S (80-1002388-08), FCX624S-HPOE-ADV (80-1002715-08), FCX624S-F-ADV (80-1002727-07), FCX648S (80-1002392-08), FCX648S-HPOE (80-1002391-10), FCX648S-HPOE-ADV (80-1002716-10), FCX-2XG (80-1002399-01)], [ICX 6610-24F-I (80-1005350-04), ICX 6610-24F-E (80-1005345-04), ICX 6610-24-I (80-1005348-05), ICX 6610-24-E (80-1005343-05), ICX 6610-24P-I (80-1005349-06), ICX 6610-24P-E (80-1005344-06), ICX 6610-48-I (80-1005351-05), ICX 6610-48-E (80-1005346-05), ICX 6610-48P-I (80-1005352-06), ICX 6610-48P-E (80-1005347-06)], [ICX 6450-24P (80-1005996-04), ICX 6450-24 (80-1005997-03), ICX 6450-48P (80-1005998-04), ICX 6450-48 (80-1005999-04), ICX 6450-C12-PD (80-1007578-01)], [ICX7750-48F (80-1007607-01), ICX7750-48C (80-1007608-01), ICX7750-26Q (80-1007609-01), with Components (80-1007871-01; 80-1007870-01; 80-1007872-01; 80-1007873-01; 80-1007738-01; 80-1007737-01; 80-1007761-01; 80-1007760-01; 80-1007632-01)], [ICX-7450-24 (80-1008060-01), ICX-7450-24P (80-1008061-01), ICX-7450-48 (80-1008062-01), ICX-7450-48P (80-1008063-01), ICX-7450-48F (80-1008064-01), with Components (123400000829A-R01; 123400000830A-R01; 123400000833A-R01; 80-1008334-01; 80-1008333-01; 80-1008332-01; 80-1008331-01; 80-1005261-04; 80-1005259-04; 80-1005262-03; 80-1005260-03; 80-1007165-03; 80-1007166-03; 80-1008308-01; 80-1008309-01)], [FI-SX800-S (80-1003050-03; 80-1007143-03), FI-SX1600-AC (80-1002764-02; 80-1007137-02), FI-SX1600-DC (80-1003005-02; 80-1007138-02), with Components (80-1002957-03; 80-1006486-02; 80-1007350-02; 80-1006607-01; 80-1007349-01; 80-1003883-02; 80-1003886-02; 11456-005; 11457-006; 18072-004)]} with FIPS Kit XBR-000195 (80-1002006-02); Firmware Version: IronWare R08.0.20a
2531	01/11/2016	McAfee Web Gateway WG5000 and WG5500 Appliances	Intel Corporation	Hardware Version: 5000 with EWG-5000-FIPS-KIT and 5500 with EWG-5500-FIPS-KIT; Firmware Version: 7.3.2.3.4
2533	01/12/2016	Brocade(R) MLXe(R) NetTron(R) Ethernet Routers	Brocade Communications Systems, Inc.	Hardware Version: {[BR-MLXE-4-MR2-M-AC (80-1006870-01), BR-MLXE-4-MR2-M-DC (80-1006872-01), BR-MLXE-8-MR2-M-AC (80-1007225-01), BR-MLXE-8-MR2-M-DC (80-1007226-01), BR-MLXE-16-MR2-M-AC (80-1006827-02), BR-MLXE-16-MR2-M-DC (80-1006828-02), BR-MLXE-4-MR2-X-AC (80-1006874-03), BR-MLXE-4-MR2-X-DC (80-1006875-03), BR-MLXE-8-MR2-X-AC (80-1007227-03), BR-MLXE-8-MR2-X-DC (80-1007228-03), BR-MLXE-16-MR2-X-AC (80-1006829-04), BR-MLXE-16-MR2-X-DC (80-1006834-04)] with Component P/Ns 80-1005643-01, 80-1003891-02, 80-1002983-01, 80-1003971-01, 80-1003972-01, 80-1003811-02, 80-1002756-03, 80-1004114-01, 80-1004113-01, 80-1004112-01, 80-1004760-02, 80-1006511-02, 80-1004757-02, 80-1003009-01, 80-1003052-01, 80-1003053-01, 80-1005644-03, 80-1007878-02, 80-1007911-02, 80-1007879-02} with FIPS Kit XBR-000195; Firmware Version: Multi-Service IronWare R05.8.00a

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2534	01/14/2016	Push To Talk Client Crypto Module	Kodiak Networks, Inc.	Software Version: 3.6.0
2538	01/19/2016	Brocade(R) 7840 Extension Switch	Brocade Communications Systems, Inc.	Hardware Version: {7840 Extension Switch (P/N 80-1008000-01)} with FIPS Kit P/N Brocade XBR-000195; Firmware Version: Fabric OS v7.4.0 (P/N 51-1001672-01)
2539	01/25/2016	FortiMail 5.2	Fortinet Inc.	Firmware Version: FortiMailOS 5.2, build0460,150922
2540	01/25/2016	FortiMail-1000D and FortiMail-3000D	Fortinet Inc.	Hardware Version: Fortimail-1000D: C1AA85 with Disk Trays P/N: SP-D2000 and Power Supplies P/N: SP-FXX1000D-PS, FortiMail-3000D: C1AA63 with Disk Trays P/N: SP-D2TC and Power Supplies P/N: D750E-S1, Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiMailOS 5.2, build0460,150922
2541	01/26/2016	VERN (TM) RMW Crypto Library	Relocation Management Worldwide	Software Version: 1.2
2542	01/26/2016	FortiClient 5.0 VPN Client	Fortinet Inc.	Software Version: FortiClient 5.0, build0367, 151201
2543	01/26/2016	FortiClient 5.0 VPN Client	Fortinet Inc.	Software Version: FortiClient 5.0, build0367, 151201
2544	01/26/2016	HID Global ActivID Applet Suite v2.7.3 on Giesecke & Devrient Sm@rtCafé Expert 7.0	HID Global and Giesecke & Devrient	Hardware Version: SLE78CLFX4000P(M) M7892; Firmware Version: Sm@rtCafé Expert 7.0 and HID Global ActivID Applet Suite 2.7.3
2545	01/26/2016	HID Global ActivID Applet Suite v2.7.3 on Oberthur Technologies Cosmo V8	HID Global and Oberthur Technologies	Hardware Version: Oberthur Technologies '0F'; Firmware Version: Oberthur Technologies '5601' and HID Global ActivID Applet Suite 2.7.3
2546	01/26/2016	CN1000/CN3000 Series Encryptors	Senetas Corporation Ltd. and SafeNet Inc.	Hardware Version: Senetas Corp. Ltd. CN1000 Series: A5141B (AC); CN3000 Series: A5203B (AC) and A5204B (DC); Senetas Corp. Ltd. & SafeNet Inc. CN1000 Series: A5141B (AC); CN3000 Series: A5203B (AC) and A5204B (DC); Firmware Version: 4.6.1
2547	01/28/2016	Motorola Solutions Astro Subscriber uMACE - Level 2	Motorola Solutions, Inc.	Hardware Version: AT8358Z04; Firmware Version: R01.06.57 and [R01.00.02 or (R01.00.02 and R01.00.03)]
2548	01/28/2016	RS9113	Redpine Signals, Inc.	Hardware Version: 6.0; Firmware Version: RS9113.N00.WC.FIPS.OSI.1.2.6 with Bootloader version 1.7
2549	01/29/2016	SUSE Linux Enterprise Server 12 - Kernel Crypto API Cryptographic Module	SUSE, LLC	Software Version: 1.0
2550	01/29/2016	McAfee Linux Cryptographic Module	Intel Corporation	Software Version: 1.0.1