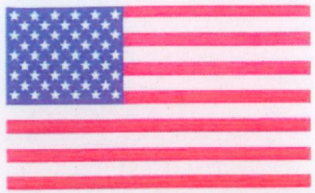
FIPS 140-2 Consolidated Validation Certificate



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

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0024

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: 1/8/13

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 7 January 2013

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
1800	12/06/2012	eToken 4300	SafeNet, Inc.	Hardware Version: Inside Secure AT90SC28880RCFV Rev. G; Firmware Version: SafeNet eToken 4300 010E.1245.0002 with PIV Applet 3.0
1820	12/05/2012	Aruba AP-120 Series and Dell W-AP120 Series Wireless Access Points	Aruba Networks, Inc.	Hardware Versions: AP-124-F1 [1], AP-125-F1 [1], W-AP124-F1 [2] and W-AP125-F1 [2] with FIPS kit 4010061-01; Firmware Versions: ArubaOS_6.1.2.3-FIPS [1] and Dell_PCW_6.1.2.3-FIPS [2]
1846	12/19/2012	McAfee Firewall Enterprise 1100E	McAfee, Inc.	Hardware Version: NSA-1100-FWEX-E and FRU-686-0089-00; Firmware Versions: 7.0.1.03 and 8.2.0
1847	12/19/2012	McAfee Firewall Enterprise 2150E	McAfee, Inc.	Hardware Version: NSA-2150-FWEX-E and FRU-686-0089-00; Firmware Versions: 7.0.1.03 and 8.2.0
1848	12/19/2012	McAfee Firewall Enterprise 4150E	McAfee, Inc.	Hardware Version: NSA-4150-FWEX-E and FRU-686-0089-00; Firmware Versions: 7.0.1.03 and 8.2.0
1849	12/06/2012	Aruba AP-60 and AP-61 Wireless Access Points	Aruba Networks, Inc.	Hardware Versions: AP-60-F1 Rev. 01 and AP-61-F1 Rev. 01 with FIPS kit 4010061-01; Firmware Version: ArubaOS_6.1.2.3-FIPS
1859	12/03/2012	Red Hat Enterprise Linux 6.2 Openswan Cryptographic Module	Red Hat®, Inc.	Software Version: 2.0
1861	12/10/2012	RSA BSAFE® Crypto-C Micro Edition for Samsung MFP SW Platform (VxWorks)	RSA Security, Inc.	Software Version: 3.0.0.1
1863	12/13/2012	Virtual System Administrator Cryptographic Module	Kaseya US Sales, LLC	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1865	12/18/2012	Aruba 3000 [A], 6000/M3 Revision C4 [B] and Dell W-3000 [C], W-6000M3 [D] Controllers with ArubaOS FIPS Firmware	Aruba Networks, Inc.	Hardware Versions: [3200-F1 Revision C4, 3400-F1 Revision C4, 3600-F1 Revision C4, 3200-USF1 Revision C4, 3400-USF1 Revision C4 and 3600-USF1 Revision C4] [1] [A], [(6000-400-F1 or 6000-400-USF1) with M3mk1-S-F1 Revision C4, HW-FT, HW-PSU-200 or HW-PSU-400, LC-2G-1, LC-2G24F-1 or LC-2G24FP-1] [1] [B], [W-3200-F1, W-3400-F1, W-3600-F1, W-3200-USF1, W-3400-USF1 and W-3600-USF1] [2] [C], and [(W-6000-400-F1 or W-6000-400-USF1) with W-6000M3, HW-FT and HW-PSU-400] [2] [D] with FIPS kit 4010061-01; Firmware Version: ArubaOS_MMC_6.1.2.3-FIPS [1] and Dell_PCW_MMC_6.1.2.3-FIPS [2]
1866	12/19/2012	FortiGate-3950B/3951B	Fortinet, Inc.	Hardware Versions: FortiGate-3950B (C4DE23) and FortiGate-3951B [(C4EL37) and FSM-064 (PE4F79)] with Blank Face Plate (P06698-02) and Tamper Evident Seal: FIPS-SEAL-RED; Firmware Version: FortiOS 4.0, build8892, 111128
1867	12/19/2012	Cygnus X3 Hardware Security Module (XHSM)	Pitney Bowes Inc.	Hardware Version: P/N 1R84000 Version A; Firmware Versions: 01.00.06 and 01.03.0074 (Device Abstraction Layer)

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1869	12/21/2012	XTM 21 [1], XTM 21-W [2], XTM 22 [3], XTM 22-W [4], XTM 23 [5], XTM 23-W [6], XTM 25 [7], XTM 25-W [8], XTM 26 [9], XTM 26-W [10], XTM 33 [11], XTM 33-W [12], XTM 330 [13], XTM 505 [14], XTM 510 [15], XTM 520 [16], XTM 530 [17], XTM 810 [18], XTM 820 [19], XTM 830 [20], XTM 830-F [21], XTM 1050 [22] and XTM 2050 [23]	WatchGuard Technologies, Inc.	Hardware Versions: XP3E6 [1, 3, 5], XP3E6W [2, 4, 6], FS1E5 [7, 9], FS1E5W [8, 10], FS2E5 [11], FS2E5W [12], NC5AE7 [13], NC2AE8 [14, 15, 16, 17], NS2BE10 [18, 19, 20], NS2BE6F4 [21], NX3CE12 [22] and NC4E16F2 [23] with Tamper Evident Seal Kit: SKU WG8566; Firmware Version: Fireware XTM OS v11.5.1