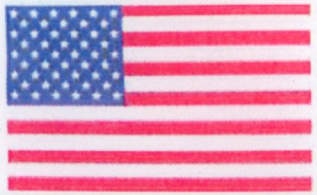
FIPS 140-2 Consolidated Validation Certificate



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. 25

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: 2/19/2013

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Scott Anderson

Dated: Feb 7, 2013

A/Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1825	01/25/2013	LogLogic Communications Cryptographic Module	TIBCO LogLogic®, Inc.	Software Version: 1.0
1833	01/07/2013	Fusion 802.1x Authentication Supplicant	Motorola Solutions, Inc.	Software Version: H_3.40.0.0.19
1855	01/18/2013	Nexus FIPS 140-2 Crypto Module	Nexus Wireless	Hardware Version: 1.01; Firmware Versions: ES0408_RL01_R1_02_001 version 1.02.001 and ES0408_RL02_R1_02_000 version 1.02.000
1860	01/25/2013	CE Secure	CMS Products	Hardware Versions: P/Ns CE-HDDFIPS-500, CE-HDDFIPS-320 and CE-HDDFIPS-250; Firmware Version: 0001SDM7
1862	01/07/2013	Seagate Secure® TCG Enterprise SSC Pulsar.2 Self-Encrypting Drive FIPS 140 Module	Seagate Technology LLC	Hardware Version: 1BU282; Firmware Version: 0003
1868	01/15/2013	B200™, B300™ and B400™ Remote Support Appliances	Bomgar Corporation	Hardware Versions: B200 [1], B300r1 [2] and B400r1 [3]; Tamper Evident Label Kit: TEL135325 [1,2,3]; Front Bezels: (FB000300 [2] and FB000400 [3]); Software Version: 12.1.6FIPS; Firmware Version: 3.3.2FIPS
1870	01/08/2013	McAfee Firewall Enterprise 1100F	McAfee, Inc.	Hardware Version: NSA-1100-FWEX-F and FIPS Kit: SAC-1100F-FIPS-KT; Firmware Version: 7.0.1.03 and 8.2.0
1871	01/08/2013	McAfee Firewall Enterprise 2150F	McAfee, Inc.	Hardware Version: NSA-2150-FWEX-F and FIPS Kit: SAC-2150F-FIPS-KT; Firmware Version: 7.0.1.03 and 8.2.0
1872	01/08/2013	McAfee Firewall Enterprise 4150F	McAfee, Inc.	Hardware Version: NSA-4150-FWEX-FRR and FIPS Kit: SAC-4150F-FIPS-KT; Firmware Version: 7.0.1.03 and 8.2.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1873	01/08/2013	datAshur Secure USB Flash Drive	iStorage Limited	Hardware Version: IS-FL-DA-256-4 [1], IS-FL-DA-256-8 [2] and IS-FL-DA-256-16 [3]; Firmware Version: V01.12A13-F05 [1], V01.12A13-F04 [2] and V01.12A15 Code Package-111130 [3] with Security Controller Firmware Revision iStorage v6
1874	01/18/2013	IMB-1000 HFR and IMB-1200 HFR Secure Media Blocks	Ultra Stereo Labs, Inc.	Hardware Versions: Rev. 11 and 12; Firmware Version: 08162012
1875	01/25/2013	Cisco Catalyst 6506, 6506-E, 6509, and 6509-E Switches with Wireless Services Modules (WiSMs)	Cisco Systems, Inc.	Hardware Versions: Chassis: Catalyst 6506 switch [1], Catalyst 6506-E switch [2], Catalyst 6509 switch [3] and Catalyst 6509-E switch [4]; Backplane: WS-C6506 [1], WS-C6506-E [2], WS-C6509 [3] and WS-C6509-E [4]; FIPS Kit: P/N 800-27009 [1, 2] and P/N 800-26335 [3, 4]; Supervisor Blade [1, 2, 3, 4]: [WS-SUP720-3BXL or WS-SUP720-3B] and WiSM: WS-SVC-WISM-1-K9; Firmware Versions: Supervisor Blade: Cisco IOS Release 12.2.33-SXI3 or Cisco IOS Release 12.2.33-SXH5; WiSM: 7.0.230.0
1876	01/30/2013	Apricorn Aegis Secure Key	Apricorn Inc.	Hardware Versions: ASK-256-4GB [1], ASK-256-8GB [2] and ASK-256-16GB [3]; Firmware Versions: V01.12A13-F05 [1], V01.12A13-F04 [2] and V01.12A15 Code Package-111130 [3] with Security Controller Firmware Revision iStorage v6

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1877	01/30/2013	PA-500, PA-2000 Series, PA-4000 Series, and PA-5000 Series Firewalls	Palo Alto Networks	Hardware Versions: HW P/Ns 910-000006-00H Rev. H with FIPS Kit P/N 920-000005-004 Rev. 4 (PA-500), 910-000004-00Q Rev. Q with FIPS Kit P/N 920-000004-004 Rev. 4 (PA-2020), 910-000003-00Q Rev. Q with FIPS Kit P/N 920-000004-004 Rev. 4 (PA-2050), 910-000002-00U Rev. U with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4020), HW P/N 910-000001-00U Rev. U with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4050), 910-000005-00L Rev. L with FIPS Kit P/N 920-000003-001 Rev. 1 (PA-4060), 910-000010-008 Rev. 8 w/ FIPS Kit P/N 920-000037-002 Rev. 2 (PA-5020), 910-000009-009 Rev. 9 w/ FIPS Kit P/N 920-000037-002 Rev. 2 (PA-5050) and 910-000008-008 Rev. 8 w/ FIPS Kit P/N 920-000037-002 Rev. 2 (PA-5060); Firmware Version: 4.0.10 or 4.0.12-h2
1878	01/31/2013	Mocana Cryptographic Suite B Module	Mocana Corporation	Software Version: 5.5f