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. 0022

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: _____

Dated: 8/11/12

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 2 Nov 2012

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
1804	10/03/2012	Diversinet Java Crypto Module for Mobile	Diversinet Corp.	Software Version: 2.0
1805	10/02/2012	LogRhythm 6.0.4 AI Engine Server	LogRhythm	Software Version: 6.0.4
1806	10/02/2012	LogRhythm 6.0.4 Windows System Monitor Agent	LogRhythm	Software Version: 6.0.4
1807	10/02/2012	LogRhythm 6.0.4 Console	LogRhythm	Software Version: 6.0.4
1808	10/02/2012	LogRhythm 6.0.4 Log Manager	LogRhythm	Software Version: 6.0.4
1809	10/02/2012	LOK-IT® 10 KEY (Series SDG003FM)	Systematic Development Group, LLC	Hardware Versions: HW003-16 Rev:03, HW003-08 Rev:02 and HW003-04 Rev:02; Firmware Version: USB Controller Firmware Revision V01.12A12-F01; Security Controller Firmware Revision SDG003FM-010
1810	10/11/2012	FortiGate-1240B [1] and FortiGate-3140B [2]	Fortinet, Inc.	Hardware Versions: C4CN43 [1] and C4XC55 [2] with Tamper Evident Seal Kit: FIPS-SEAL-BLUE [1] or FIPS-SEAL-RED [2]; Firmware Version: FortiOS 4.0, build8892, 111128
1811	10/11/2012	Diversinet Java Crypto Module	Diversinet Corp.	Software Version: 2.0
1812	10/11/2012	McAfee Firewall Enterprise Control Center Virtual Appliance	McAfee, Inc.	Software Versions: 5.2.0 and 5.2.1
1813	10/11/2012	Junos-FIPS 10.4 L2 OS Cryptographic Module	Juniper Networks, Inc.	Firmware Version: 10.4R5
1814	10/11/2012	Crypto Module C	Websense Inc.	Software Version: 1.0
1815	10/11/2012	Aruba RAP-5WN and Dell W-RAP-5WN Remote Access Points	Aruba Networks, Inc.	Hardware Versions: RAP-5WN-F1 [1] and W-RAP-5WN-F1 [2]; Firmware Version: ArubaOS_6.1.2.3-FIPS [1] and Dell_PCW_6.1.2.3-FIPS [2]

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1816	10/11/2012	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: 4.0.1
1817	10/11/2012	LogRhythm 6.0.4 Event Manager	LogRhythm	Software Version: 6.0.4
1818	10/11/2012	Cisco EX60 and EX90 TelePresence Systems	Cisco Systems, Inc.	Hardware Version: v1 with CISCO-FIPSKIT=; Firmware Version: TC5.0.2
1819	10/12/2012	Symantec Control Center Cryptographic Module	Symantec Corporation	Software Version: 1.0