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. 0013

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: 2/17/2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: February 8, 2012

A/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
1631	01/24/2012			
1645	12/15/2011	McAfee Web Gateway WG5000 and WG5500 Appliances	McAfee, Inc.	Hardware Versions: (5000 and 5500) with Part Number: 820-1919-00; Firmware Version: 7.1.0
1651	01/05/2012	ecoNet smart grid gateways: ecoNet SL and ecoNet MSA	Nexgrid, LLC	Hardware Versions: ENSL2, ENSL5 and ENMSA2; Firmware Version: 3.1.2-FIPS
1663	01/05/2012			
1664	01/10/2012	Security Builder® FIPS Module	Certicom Corp.	Firmware Versions: 4.0 B and 4.0 S
1665	01/10/2012	Network Security Platform Sensor M-8000 S	McAfee, Inc.	Hardware Version: P/N M-8000 S, Version 1.40; FIPS Kit P/N IAC-FIPS-KT8; Firmware Version: 6.1.15.35
1666	01/25/2012	Motorola Mobility Cryptographic Suite B Module	Motorola Mobility, Inc.	Software Version: 5.4fm
1667	01/11/2012	Secure Media Block	Qube Cinema, Inc.	Hardware Versions: Z-OEM-DCI-Q-R0, Z-OEM-DCI-Q-R2 and Z-OEM-DCI-Q-R3; Firmware Version: 1.0.1.0
1668	01/19/2012	Cisco Common Cryptographic Module (C3M)	Cisco Systems, Inc.	Hardware Versions: Intel [Core i5, Core i7 and Xeon] with AES-NI; Software Version: 0.9.8r.1.1
1669	01/19/2012	BlackBerry Cryptographic Kernel	Research In Motion Ltd.	Firmware Versions: 3.8.7.0 [1] and 3.8.7.1 [1,2]