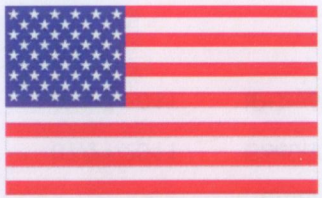
FIPS 140-2 Consolidated Validation Certificate



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. 0007

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: Don Fl

Dated: Aug 11, 2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 29 July, 2011.

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
1551	07/21/2011	Check Point IP Appliance	Check Point Software Technologies Ltd.	Hardware Versions: IP390 (CPAP-IP395-D-GFIP [Nokia NBB0302000] and N431174001) and IP560 (CPAP-IP565-D-AC [Nokia NBB0562000] and CPIP-A-4-1C, CPIP-A-PCMCIA-CA, N431174001); Firmware Version: IPSO v4.2 with Check Point VPN-1 NGX R65 with hot fix HFA-30
1569	07/11/2011	IMB	Doremi Cinema LLC	Hardware Versions: IMB-A0, IMB-A1, IMB-A2, IMB-E0, IMB-E1 and IMB-E2; Firmware Versions: 5.0.10f, 30.04m-1 and 99.03f
1571	07/13/2011	nShield Connect 6000 [1], nShield Connect 1500 [2] and nShield Connect 500 [3]	Thales - nCipher	Hardware Versions: NH2047 [1], NH2040 [2] and NH2033 [3], Build Standard N; Firmware Version: V11.30
1572	07/13/2011	Harris AES Software Load Module	Harris Corporation	Software Version: 1.0
1573	07/15/2011	PKI BLADE Applet and Protiva PIV DL Card	U.S. Department of State	Hardware Version: P/N P5CD144 Version A1047808; Firmware Version: EI08-M1004069, Softmask V01, PIV Applet V1.55 and PKI BLADE Applet V1.2
1574	07/15/2011	Endpoint Encryption Manager	McAfee, Inc.	Software Version: 5.2.6
1575	07/15/2011	BlackBerry Smartcard Reader	Research In Motion Ltd.	Hardware Version: 2.0; Firmware Version: 3.8.5.51
1576	07/21/2011	MiniCrypt	Teledyne Webb Research	Software Version: 1.2
1578	07/21/2011	BlackBerry Tablet Cryptographic Kernel	Research in Motion Ltd.	Software Version: 5.6
1579	07/21/2011	Security Builder FIPS Module	Certicom Corp.	Software Version: 5.6
1582	07/27/2011	IPCryptR2	Motorola, Inc.	Hardware Version: P/N BLN1306A; Firmware Version: R03.01.51

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1583	07/27/2011	FortiGate-200B [1], FortiGate-300A [2], FortiGate-300A-HD [3], FortiGate-310B [4], FortiGate-311B [5], FortiGate-620B [6] and FortiGate-800 [7]	Fortinet, Inc.	Hardware Versions: C4CD24 [1], C4FK88 [2], C4FK88 [3], C4ZF35 [4], C4CI39 [5], C4AK26 [6] and C4UT39 [7]; Firmware Version: FortiOS 4.0, build6359, 100712
1584	07/27/2011	FortiGate-1240B [1], FortiGate-3016B [2], FortiGate-3600A [3] and FortiGate-3810A-E4 [4]	Fortinet, Inc.	Hardware Versions: C4CN43 [1], C4XA14 [2], V3BU94 [3] and C3GV75 [4]; Firmware Version: FortiOS 4.0, build6341, 100617
1585	07/27/2011	FortiGate-80C [1], FortiGate-110C [2] and FortiGate-111C [3]	Fortinet, Inc.	Hardware Versions: C4BC61 [1], C4HA15 [2] and C4BQ31 [3]; Firmware Version: FortiOS 4.0, build6359, 100712