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. 0016

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: 7 MAY 2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____ A/DirATA

Dated: 2 May 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
1702	04/12/2012	Entrust Authority™ Security Kernel	Entrust, Inc.	Software Version: 8.1sp1
1703	04/03/2012	IntelliCom WAN 1720	S&C Electric Company	Hardware Version: IntelliCom WAN 1720; Firmware Version: 1.1.0.0
1704	04/05/2012	Juniper Networks SRX650 Services Gateways	Juniper Networks, Inc.	Hardware Versions: (SRX650-BASE-SRE6-645AP and SRX650-BASE-SRE6-645DP) with JNPR-FIPS-TAMPER-LBLS; Firmware Version: 11.2S4
1705	04/12/2012	nShield F3 500 PCI [1], nShield F3 500 for NetHSM [2] and nShield F3 10 PCI [3]	Thales-eSecurity Inc.	Hardware Versions: nC4033P-500 [1], nC4033P-500N [2] and nC4033P-10 [3], Build Standard N; Firmware Version: 2.50.16-2
1706	04/12/2012	FortiMail™ OS	Fortinet, Inc.	Firmware Version: FortiMail 4.0, build0369, 110615
1707	04/12/2012	FortiMail-3000C	Fortinet, Inc.	Hardware Version: C4GY52; Firmware Version: FortiMail 4.0, build0369, 110615
1708	04/27/2012	nShield F3 4000 [1], nShield F3 2000 [2], nShield F3 2000 for NetHSM [3], nShield F3 500 [4] and nShield F3 500 for NetHSM [5]	Thales-eSecurity Inc.	Hardware Versions: nC4033P-4K0 [1], nC4033P-2K0 [2], nC4033P-2K0N [3], nC4133P-500 [4] and nC4133P-500N [5], Build Standard N; Firmware Version: 2.50.16-3
1709	04/27/2012	HP TippingPoint Intrusion Prevention System	Hewlett-Packard TippingPoint	Hardware Version: S6100N; Firmware Version: 3.2.1.1639
1710	04/30/2012	NSS Freebl Cryptographic Module	Red Hat, Inc.	Software Version: 3.12.9.1
1711	04/30/2012	IDProtect with LASER PKI	Athena Smartcard, Inc.	Hardware Version: Inside Secure AT90SC28872RCU Rev. G; Firmware Version: Athena IDProtect 010B.0352.0005 with LASER PKI Applet 3.0