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. 0009

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: DF Boh

Dated: 14 October, 2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 3 October, 2011

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1594	9/27/2011	SafeNet Ethernet Encryptor, Branch Office	SafeNet, Inc.	Hardware Versions: 943-5020v-004 [1] [2] and 943-50211-001 [2]; Firmware Versions: 1.0.6.4 [1] and 2.0.2 [2]
1598	09/02/2011	Symantec Cross-Platform Cryptographic Module	Symantec Corporation	Software Version: 1.0
1599	09/20/2011	HardCache™-SL3/PC v2.1	STMicroelectronics, Inc.	Hardware Version: STM7007
1600	09/08/2011	IBM® z/OS® Version 1 Release 12 System SSL Cryptographic Module	IBM® Corporation	Hardware Versions: FC3863 w/System Driver Level 86E, and optional CEX3A and CEX3C [CEX3A and CEX3C are separately configured versions of 4765-001 (P/N 45D6048)]; Software Version: System SSL level HCPT3C0/JCPT3C1 w/ APAR OA34156, RACF level HRF7770 and ICSF level HCR7770 w/ APAR OA34205; Firmware Version: 4765-001 (e1ced7a0)
1601	09/08/2011	McAfee Endpoint Encryption for PCs	McAfee, Inc.	Software Version: 5.2.6
1602	09/20/2011	Juniper Networks SRX5600 and SRX5800 Services Gateways	Juniper Networks, Inc.	Hardware Versions: (SRX5600BASE-AC, SRX5600BASE-DC, SRX5800BASE-AC and SRX5800BASE-DC) with JNPR-FIPS-TAMPER-LBLS; Firmware Version: 10.4R3
1603	09/20/2011	Optical Metro 5130	Ciena® Corporation	Hardware Version: Chassis: NTB200BAE5 Rev: 03, S-DNM: NTB211AAE5 Rev: 02, Filler: NTB207BAE5 Rev: 02, and Seal Kit: NTB209LAE6; Firmware Version: 4.00.008.927
1604	09/20/2011	Centrify Cryptographic Module	Centrify Corporation	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1605	09/26/2011	CEP100, CEP100 VSE, CEP100-XSA, CEP1000, CEP1000-DP and CEP1000 VSE	Certes Networks, Inc.	Hardware Versions: [CEP100, A], [CEP100 VSE, A], [CEP100-XSA, A], [CEP1000, A], [CEP1000-DP, A] and [CEP1000 VSE, A]; Firmware Version: 1.6
1606	09/26/2011	Fortress Mesh Points	Fortress(TM) Technologies	Hardware Versions: ES210, ES300, ES440, ES520v1, ES520v2 and ES820; Firmware Version: 5.3.1
1607	09/26/2011	Verdasys Secure Cryptographic Module	Verdasys, Inc.	Software Version: 1.0
1608	09/26/2011	NonStop Volume Level Encryption (NSVLE)	Hewlett-Packard Company	Software Version: 1.0
1609	09/26/2011	SpectraGuard® Enterprise Sensor	AirTight Networks, Inc.	Hardware Version: SS-300-AT-C-10 with SS-FIPS-TPL; Firmware Version: 6.2.39p1
1610	09/26/2011	4 Gb/s FC I/O Module with Encryption	EMC Corporation	Hardware Version: 303-176-100B B04
1612	9/29/2011	Mocana Cryptographic Loadable Kernel Module	Mocana Corporation	Software Version: 5.4f
1614	9/30/2011	Mocana Cryptographic Suite B Module	Mocana Corporation	Software Version: 5.4f
1615	9/30/2011	Symantec Java Cryptographic Module	Symantec Corporation	Software Version: 1.0