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. 0010

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: Dawn F. Dodson

Dated: 8/Nov 11

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 1 NOV 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
1581	10/11/2011	Check Point IP Appliance	Check Point Software Technologies Ltd.	Hardware Versions: IP290 (CPAP-IP295-D-GFIP [Nokia NBB0292000] and N431174001, CPAP-IP295-D-AC-DS [Nokia NBB0295000] and N431174001) and IP690 (CPAP-IP695-D-GFIP [Nokia NBB0692000], CPIP-A-4-1C and N431174001); Firmware Version: IPSO v4.2 with Check Point VPN-1 NGX R65 with hot fix HFA-30
1611	10/06/2011	Juniper Networks SRX3400 and SRX3600 Services Gateways	Juniper Networks, Inc.	Hardware Versions: (SRX3400BASE-AC, SRX3400BASE-DC, SRX3600BASE-AC and SRX3600BASE-DC) with JNPR-FIPS-TAMPER-LBLS; Firmware Version: 10.4R3
1613	10/06/2011	Juniper Networks SRX100, SRX210, SRX220, SRX240 and SRX650 Services Gateways	Juniper Networks, Inc.	Hardware Versions: (SRX100B, SRX100H, SRX210B, SRX210BE, SRX210H, SRX210HE, SRX210H-POE, SRX210HE-POE, SRX220H, SRX220H-POE, SRX240B, SRX240H, SRX240H-POE, SRX650-BASE-SRE6-645AP and SRX650-BASE-SRE6-645DP) with JNPR-FIPS-TAMPER-LBLS; Firmware Version: 10.4R3
1616	10/05/2011	Concepteers Teleconsole E	Concepteers, LLC	Hardware Version: rev A1; Firmware Version: 2.0
1617	10/06/2011	Dell PowerConnect J-Series J-SRX100, J-SRX210 and J-SRX240 Services Gateways	Dell, Inc.	Hardware Versions: (J-SRX100B, J-SRX100H, J-SRX210B, J-SRX210BE, J-SRX210H, J-SRX210HE, J-SRX210H-POE, J-SRX210HE-POE, J-SRX240B, J-SRX240H and J-SRX240H-POE) with JNPR-FIPS-TAMPER-LBLS; Firmware Version: 10.4R3

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1618	10/18/2011			
1619	10/19/2011	FIPS Multi Service PIC	Juniper Networks, Inc.	Hardware Versions: PE-MS-100-1, PB-MS-100-1, PB-MS-400-2 and PC-MS-500-3; Firmware Version: 10.4 R1.9
1620	10/19/2011	KlasRouter	Klas Ltd	Hardware Version: KlasRouter, Versions 3.02 and 3.03; Firmware Version: KlasOS3, Version 3.1.0 rc0
1621	10/28/2011	Cisco 7606-S and 7609-S Routers with Supervisor SUP720-3B	Cisco Systems, Inc.	Hardware Versions: 7606-S and 7609-S with SUP720-3B; Firmware Version: 15.1(2)S
1622	10/24/2011	CEP10-R, CEP10 VSE and CEP10-C	Certes Networks, Inc.	Hardware Versions: [CEP10-R, PN 410-032-402, A], [CEP10 VSE, PN 410-032-402, A], [CEP10-C, PN 410-032-602, A] and [CEP10 VSE, PN 410-032-602, A]; Firmware Version: 1.6
1623	10/24/2011			
1624	10/24/2011			
1626	10/31/2011	FlagStone Core	ViaSat UK Ltd.	Hardware Versions: V2.0.1.1, V2.0.1.2, V2.0.1.3, V2.0.2.1, V2.0.2.2, V2.0.2.3, V2.0.3.3, V2.0.3.4, V2.0.4.5, V2.0.5.3, V2.0.5.4, and V2.0.5.5