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. 0023

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: 3 Dec 2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 3 December 2012

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1790	11/05/2012	PrivateServer	ARX (Algorithmic Research)	Hardware Version: 4.7; Firmware Version: 4.8.1
1821	11/01/2012	Crypto Dual (Underlying Steel Chassis) [1] and Crypto Dual Plus (Underlying Steel Chassis) [2]	Integral Memory PLC.	Hardware Versions: INFD2GCRYPTODL140-2(R) [1], INFD4GCRYPTODL140-2(R) [1], INFD8GCRYPTODL140-2(R) [1], INFD16GCRYPTODL140-2(R) [1], INFD32GCRYTPODL140-2(R) [1], INFD64GCRYPTODL140-2(R) [1], INFD2GCRYDLP140-2(R) [2], INFD4GCRYDLP140-2(R) [2], INFD8GCRYDLP140-2(R) [2], INFD16GCRYDLP140-2(R) [2], INFD32GCRYDLP140-2(R) [2], INFD64GCRYDLP140-2(R) [2], INFD128GCRYDLP140-2(R) [2], INFD256GCRYDLP140-2(R) [2], INFD512GCRYDLP140-2(R) [2] and INFD1TCRYDLP140-2(R) [2]; Firmware Version: PS2251-65
1822	11/01/2012	iButton Postal Security Device	Data-Pac Mailing Systems Corp.	Hardware Version: MAXQ1959B-F50#; Firmware Version: 1.3
1823	11/05/2012	Cisco Telepresence C40, C60, and C90 Codecs	Cisco Systems, Inc.	Hardware Version: v1 with CISCO-FIPSKIT=; Firmware Version: TC5.0.2
1824	11/14/2012	Cisco Telepresence C20 Codec	Cisco Systems, Inc.	Hardware Version: v1; Firmware Version: TC5.0.2
1826	11/05/2012	Seagate Secure® TCG Opal SSC Self-Encrypting Drive	Seagate Technology LLC	Hardware Versions: 9WU142, 9WU14C and 9WU141; Firmware Version: 0001SDM7 or 0001SED7
1827	11/05/2012	Symantec Scanner Cryptographic Module	Symantec Corporation	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1828	11/05/2012	Aruba AP-134, AP-135 and Dell W-AP134, W-AP135 Wireless Access Points	Aruba Networks, Inc.	Hardware Versions: AP-134-F1 [1], AP-135-F1 [1], W-AP134-F1 [2] and W-AP135-F1 [2] with FIPS kit 4010061-01; Firmware Version: ArubaOS_6.1.2.3-FIPS [1] and Dell_PCW_6.1.2.3-FIPS [2]
1829	11/05/2012	Cisco 5508 Wireless LAN Controller	Cisco Systems, Inc.	Hardware Version: CT5508 Revision Number B0; FIPS Kit AIR-CT5508FIPSKIT=; Opacity Baffle Version A0; Firmware Version: 7.0.230.0 or 7.2.103.0
1830	11/05/2012	FortiGate-5140 Chassis with FortiGate 5000 Series Blades	Fortinet, Inc.	Hardware Version: Chassis: C4GL51; Blades: P4CF76, P4CJ36-02, P4CJ36-04 and P4EV74; AMC Components: P4FC12 and AMC4F9; Shelf Manager: PN 21594 346; Alarm Panel: PN 21594 159; Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 4.0, build8892, 111128
1831	11/05/2012	KMF CryptR	Motorola Solutions, Inc.	Hardware Version: P/N CLN8566A; Firmware Version: R01.02.10
1832	11/07/2012	FortiGate-60C [1], FortiGate-110C [2] and FortiGate-111C [3]	Fortinet, Inc.	Hardware Versions: C4DM93 [1], C4HA15 [2] and C4BQ31 [3] with Tamper Evident Seal Kit: FIPS-SEAL-RED [1] or FIPS-SEAL-BLUE [2,3]; Firmware Version: FortiOS 4.0, build8892, 111128
1834	11/08/2012	FortiGate-200B [1], FortiGate-310B [2] and FortiGate-620B [3]	Fortinet, Inc.	Hardware Versions: C4CD24 [1], C4ZF35 [2] and C4AK26 [3] with Tamper Evident Seal Kit: FIPS-SEAL-BLUE; Firmware Version: FortiOS 4.0, build8892, 111128

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1835	11/08/2012	NITROX XL 1600-NFBE HSM Family	Cavium Networks	Hardware Version: P/Ns CN1620-NFBE1NIC-2.0, CN1620-NFBE3NIC-2.0, CN1610-NFBE1NIC-2.0, CN1610-NFBE1-3.0, CN1620-NFBE1-3.0, CN1620-NFBE3-3.0, CN1610-NFBE1-2.0, CN1620-NFBE1-2.0 and CN1620-NFBE3-2.0; Firmware Version: CN16XX-NFBE-FW-2.1-110015
1836	11/08/2012	RSA BSAFE® Crypto-C Micro Edition for MFP SW Platform (pSOS)	RSA Security, Inc.	Software Version: 3.0.0.1 and 3.0.0.2
1837	11/08/2012	NSS Cryptographic Module	Red Hat, Inc.	Software Version: 3.12.9.1
1838	11/08/2012	Aruba AP-92, AP-93, AP-104, AP-105, AP-175, Dell W-AP92, W-AP93, W-AP104, W-AP105 and W-AP175 Wireless Access Points	Aruba Networks, Inc.	Hardware Versions: AP-92-F1[1], AP-93-F1[1], AP-104-F1[1], AP-105-F1[1], AP-175P-F1[1], AP-175AC-F1[1], AP-175DC-F1[1], W-AP92-F1[2], W-AP93-F1[2], W-AP104-F1[2], W-AP105-F1[2], W-AP175P-F1[2], W-AP175AC-F1[2], W-AP175DC-F1[2] with FIPS kit 4010061-01; Firmware Versions: ArubaOS_6.1.2.3-FIPS[1] and Dell_PCW_6.1.2.3-FIPS[2]
1839	11/29/2012	Entrust Authority™ Security Toolkit for the Java®Platform	Entrust, Inc.	Software Version: 8.0
1841	11/29/2012	InZero Gateway	InZero Systems	Hardware Version: XB2CUSB3.1; Firmware Version: 2.80.0.38
1842	11/29/2012	SRA EX6000 and SRA EX7000	SonicWALL, Inc.	Hardware Version: P/Ns 101-500210-62 Rev. A (SRA EX6000) and 101-500188-62 Rev. A (SRA EX7000); Firmware Version: SRA 10.6.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1843	11/29/2012	Protiva+ PIV v2.0 using TOP DL v2 and TOP IL v2	Gemalto	Hardware Version: A1025258 and A1023393; Firmware Version: Build#11 - M1005011 + Softmask V04, Applet Version: PIV Applet v2.00 + OATH Applet v2.10
1845	11/29/2012	Aruba AP-65, AP-70 and AP-85 Wireless Access Points	Aruba Networks, Inc.	Hardware Version: AP-65-F1 Rev. 01, AP-70-F1 Rev. 01, AP-85FX-F1 Rev. 01, AP-85LX-F1 Rev. 01 and AP-85TX-F1 Rev. 01 with FIPS kit 4010061-01; Firmware Version: ArubaOS_6.1.2.3-FIPS
1850	11/29/2012	RSA BSAFE® Crypto-C Micro Edition	RSA, The Security Division of EMC	Software Version: 3.0.0.16
1851	11/29/2012	McAfee Firewall Enterprise Control Center	McAfee, Inc.	Hardware Version: [FWE-C1015 and FIPS Kit: FWE-CC-FIPS-KIT1], [FWE-C2050 and FIPS Kit: FWE-CC-FIPS-KIT2] and [FWE-C3000 and FIPS Kit: FWE-CC-FIPS-KIT2]; Firmware Version: 5.2.0
1852	11/29/2012	FortiWiFi-60C	Fortinet, Inc.	Hardware Version: C4DM95 with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiOS 4.0, build8892, 111128
1853	11/29/2012	Cisco 4402 and 4404 Wireless LAN Controllers	Cisco Systems, Inc.	Hardware Version: 4402, Revision Number R0 and 4404, Revision Number R0; FIPS Kit AIRWLC4400FIPSKIT=, Version A0; Opacity Baffle Version 1.0; Firmware Version: 7.0.230.0
1856	11/29/2012	Luna® PCI 7000 for Luna® SA, Luna® PCI 7000 for Luna® SP and Luna® PCI 7000 for Luna® XML Cryptographic Modules	SafeNet, Inc.	Hardware Version: VBD-03-0100; Firmware Version: 4.8.7
1857	11/29/2012	Luna® PCI 7000 Cryptographic Module	SafeNet, Inc.	Hardware Version: VBD-03-0100; Firmware Version: 4.8.7
1858	11/29/2012	Cryptographic Security Kernel	Vidyo, Inc.	Software Version: 1.0