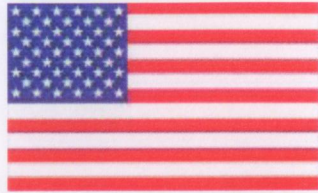
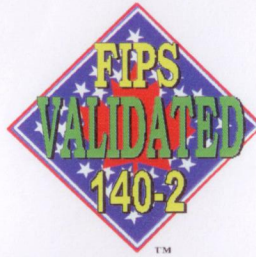


# FIPS 140-2 Consolidated Validation Certificate



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. 0019

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: 13 AUG 2012

Chief, Computer Security Division  
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: \_\_\_\_\_  
Dated: 7 Aug 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
1714	07/11/2012	Scanning and Mobility FIPS Module	Honeywell Scanning and Mobility (HSM) - USA	Firmware Versions: 4.0 B and 4.0 S
1727	07/24/2012	Aruba 620, 650 and Dell W-620, W-650 Controllers with ArubaOS FIPS Firmware	Aruba Networks	Hardware Versions: 620-F1 [1], 620-USF1 [1], 650-F1 [1], 650-USF1 [1], W-620-F1 [2], W-620-USF1 [2], W-650-F1 [2], W-650-USF1 [2] with FIPS kit 4010061-01; Firmware Versions: ArubaOS_6xx_6.1.2.3-FIPS [1] and Dell_PCW_6xx_6.1.2.3-FIPS [2]
1749	07/17/2012	IDProtect Duo with LASER PKI	Athena Smartcard, Inc.	Hardware Version: Inside Secure AT90SC28880RCFV Rev. G; Firmware Version: Athena IDProtect 010E.1245.0002 with LASER PKI Applet 3.0
1750	07/17/2012	IDProtect Key with LASER PKI	Athena Smartcard, Inc.	Hardware Version: Inside Secure AT90SC25672RCT-USB Rev. D packaged in TIDPTMINI72 and TIDPUSBV2J; Firmware Version: Athena IDProtect 0106.0130.0401 with LASER PKI Applet 3.0
1753	07/24/2012	SafeGuard® CryptoServer Se	Utimaco Safeware AG	Hardware Version: P/N CryptoServer Se, Version 3.00.3.1; Firmware Version: 1.0.1.0
1754	07/17/2012	FortiOS™	Fortinet, Inc.	Firmware Version: 4.0 MR3
1755	07/27/2012	NetScreen-5200 [1] and Netscreen-5400 [2]	Juniper Networks, Inc.	Hardware Versions: [(NS-5200 [1] with one NS-5000-8G2) and (NS-5400 [2] with one to three NS-500-8G2)] with (NS-5000-MGT2 or NS-5000-MGT3) and JNPR-FIPS-TAMPER-LBLS; Firmware Version: ScreenOS 6.3r6



Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1756	07/27/2012	NetScreen-ISG 1000 [1] and NetScreen-ISG 2000 [2]	Juniper Networks, Inc.	Hardware Versions: [NS-ISG-1000, NS-ISG-1000-DC, NS-ISG-1000B and NS-ISG-1000B-DC] [1] and [(NS-ISG-2000, NS-ISG-2000-DC, NS-ISG-2000B and NS-ISG-2000B-DC) with 1, 2, 3 or 4 FE8 Interface Cards][2] with JNPR-FIPS-TAMPER-LBLS; Firmware Version: ScreenOS 6.3r6
1757	07/27/2012	Red Hat Enterprise Linux 6.2 Libcrypt Cryptographic Module	Red Hat®, Inc.	Software Version: 2.0
1758	07/27/2012	Red Hat Enterprise Linux 6.2 OpenSSL Cryptographic Module	Red Hat®, Inc.	Software Version: 2.0
1759	07/27/2012	Cummings Engineering's Secure Mobility Suite B Crypto Module v1.0	Cummings Engineering Consultants, Inc.	Software Version: v1.0
1760	07/27/2012	Catbird vSecurity Crypto Module v1.0	Catbird Networks, Inc.	Software Version: v1.0
1761	07/27/2012	Motorola PTP 600 Series Point to Point Wireless Ethernet Bridges	Motorola Solutions, Inc.	Hardware Versions: P/Ns BP5830BHC, BP5830BHC15, BP5530BHC, BP5530BHC15, WB2781, WB3039, WB3037, WB3092, WB3094, WB3387, WB3389, WB3222, BP5830BH, BP5830BH15, BP5530BH, BP5530BH15, WB2780, WB3036, WB3038, WB3091, WB3093, WB3386, WB3388 and WB3221; with P/N WB3593 (HW Security Upgrade Kit); Firmware Version: PTP600 10-00
1762	07/27/2012	VaultIC™ 420, VaultIC™ 440 and VaultIC™ 460	INSIDE Secure	Hardware Versions: P/N: ATVaultIC420, ATVaultIC440 and ATVaultIC460, Platform: AT90SO128 - Silicon Rev C; Firmware Version: 1.2.1



Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1763	07/27/2012	Motorola PTP 800 Series CMU Cryptographic Module	Motorola Solutions, Inc.	Hardware Version: P/N WB3517, Versions 5.2, 5.3 and 6.6; Firmware Version: PTP 800 04-10
1765	07/31/2012	BlackBerry Cryptographic Java Module	Research In Motion Ltd.	Software Version: 2.8
1766	07/27/2012	ProxySG 9000-10 [1], 9000-20 [2] and 9000-20B [3]	Blue Coat Systems, Inc.	Hardware Version: 090-02844 [1], 090-02843 [1], 090-02840 [2], 090-02839 [2], 090-02984 [3] and 090-02985 [3] with FIPS kit 085-02718; Firmware Version: 6.1
1767	07/27/2012	ProxySG 900-10 [1], 900-10B [2], 900-20 [3], 900-30 [4] and 900-45 [5]	Blue Coat Systems, Inc.	Hardware Version: 090-02900 [1], 090-02901 [1], 090-02988 [2], 090-02989 [2], 090-02902 [3], 090-02903 [3], 090-02904 [4], 090-02905 [4], 09002908 [5] and 090-02909 [5] with FIPS kit 085-02742; Firmware Version: 6.1
1768	07/27/2012	ProxySG 9000-10 [1], 9000-20 [2] and 9000-20B [3]	Blue Coat Systems, Inc.	Hardware Version: 090-02844 [1], 090-02843 [1], 090-02840 [2], 090-02839 [2], 090-02984 [3] and 090-02985 [3] with FIPS kit 085-02718;; Firmware Version: 5.5



Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1769	07/27/2012	HP 5406 zl [1], HP 5412 zl [2], HP 8206 zl [3] and HP 8212 zl [4] Switches with the HP MSM765zl Mobility Controller	Hewlett-Packard Development Company, L.P.	Hardware Version: (J8697A [1], J8698A [2], J9447A [3] and J9091A [4] [B]); Management Modules: (J8726A [1,2] and J9092A [3,4] [B]); Power Supply: (J9306A: one [1,3] or two [2,4]); Support Module: (J9095A [3,4] [B]); Fabric Module: (J9093A: two [3,4] [B]); Blank Plate: (5069-8563: four [1], ten [2], five [3] or eleven [4]); Opacity Shield Kits: (J9710A [1], J9711A [2], J9712A [3] and J9713A [4]); High Performance Fan Trays: (J9721A [1], J9722A [2], J9723A [3] and J9724A [4]); with (HP Gig-T/SFP+ V2 zl Mod: J9536A; HP Mobility Controller: J9370A [A] and Tamper Evident Seal Kit: J9709A) [1,2,3,4]; Firmware Version: 5.6.0 [A] and K.15.07.0003 [B]
1770	07/31/2012	ProxySG 510-5 [1], 510-10 [2], 510-20 [3], 510-25 [4], 810-5 [5], 810-10 [6], 810-20 [7], 810-25 [8]	Blue Coat Systems, Inc.	Hardware Versions: 090-02760 Rev U.0 [1]; 090-02761 Rev X.0 [2]; 090-02762 Rev W.0 [2]; 090-02761 Rev C.0 [2]; 090-02762 Rev C.0 [2]; 090-02763 Rev W.0 [3]; 090-02764 Rev W.0 [3]; 090-02763 Rev C.0 [3]; 090-02764 Rev C.0 [3]; 090-02781 Rev X.0 [4]; 090-02782 Rev X.0 [4]; 090-02781 Rev C.0 [4]; 090-02782 Rev C.0 [4]; 090-02765 Rev W.0 [5]; 090-02766 Rev Y.0 [6]; 090-02767 Rev Y.0 [6]; 090-02766 Rev H.0 [6]; 090-02767 Rev H.0 [6]; 090-02768 Rev X.0 [7]; 090-02769 Rev X.0 [7]; 090-02768 Rev H.0 [7]; 090-02769 Rev H.0 [7]; 090-02783 Rev Z.0 [8]; 090-02784 Rev Z.0 [8]; 090-02783 Rev H.0 [8] and 090-02784 Rev H.0 [8] with FIPS kit 085-02597; Firmware Version: 6.1



Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1771	07/31/2012	ProxySG 510-5 [1], 510-10 [2], 510-20 [3], 510-25 [4], 810-5 [5], 810-10 [6], 810-20 [7] and 810-25 [8]	Blue Coat Systems, Inc.	Hardware Versions: 090-02760 Rev U.0 [1]; 090-02761 Rev X.0 [2]; 090-02762 Rev W.0 [2]; 090-02761 Rev C.0 [2]; 090-02762 Rev C.0 [2]; 090-02763 Rev W.0 [3]; 090-02764 Rev W.0 [3]; 090-02763 Rev C.0 [3]; 090-02764 Rev C.0 [3]; 090-02781 Rev X.0 [4]; 090-02782 Rev X.0 [4]; 090-02781 Rev C.0 [4]; 090-02782 Rev C.0 [4]; 090-02765 Rev W.0 [5]; 090-02766 Rev Y.0 [6]; 090-02767 Rev Y.0 [6]; 090-02766 Rev H.0 [6]; 090-02767 Rev H.0 [6]; 090-02768 Rev X.0 [7]; 090-02769 Rev X.0 [7]; 090-02768 Rev H.0 [7]; 090-02769 Rev H.0 [7]; 090-02783 Rev Z.0 [8]; 090-02784 Rev Z.0 [8]; 090-02783 Rev H.0 [8] and 090-02784 Rev H.0 [8] with FIPS kit 085-02597; Firmware Version: 5.5
1772	07/31/2012	Junos-FIPS 10.4 L1 OS Cryptographic Module	Juniper Networks, Inc.	Firmware Version: 10.4R5