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. 0026

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: Michael J Cooper

Dated: 3/19/2013

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 12 March 2013

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1840	02/11/2013	Aruba 3000 [1] and 6000/M3 Revision B2 [2] Controllers with ArubaOS FIPS Firmware	Aruba Networks, Inc.	Hardware Versions: [3200-F1 Revision B2, 3400-F1 Revision B2, 3600-F1 Revision B2, 3200-USF1 Revision B2, 3400-USF1 Revision B2, 3600-USF1 Revision B2] [1] and [(6000-400-F1 or 6000-400-USF1) with (M3mk1-S-F1 Revision B2, LC-2G-1, LC-2G24F-1, LC-2G24FP-1, HW-FT, HW-PSU-200 or HW-PSU-400] [2] with FIPS kit 4010061-01; Firmware Version: ArubaOS_MMC_6.1.2.3-FIPS
1864	02/04/2013	Cambium Networks PTP 800 Compact Modem Unit (CMU)	Cambium Networks, Ltd.	Hardware Versions: P/N WB3517, Versions 5.2, 5.3 and 6.6; Firmware Version: PTP 800-05-02
1879	02/04/2013	PoliWall-CCF M10 [1], M50 [2], G01 [3] and G10 [4] Series Security Appliance	TechGuard Security	Hardware Versions: PW-CCF-M10-01C [1], PW-CCF-M50-01C [2], PW-CCF-G01-01C [3], PW-CCF-G01-01F [3], PW-CCF-G10-01X [4] and PW-CCF-G10-01F [4] with FIPS Kits: (PW-CCF-M10-FK1 [1,2], PW-CCF-G01-FK1 [3] and PW-CCF-G10-FK1 [4]); Software Version: 2.02.3101
1880	02/04/2013	SecureDoc® Disk Encryption Cryptographic Engine for Windows	WinMagic Inc.	Software Version: 6.1
1881	02/04/2013	SecureDoc® Disk Encryption Cryptographic Engine for MacOS X	WinMagic Inc.	Software Version: 6.1
1882	02/08/2013	Entrust IdentityGuard PIV Credential	Entrust, Inc.	Hardware Version: SCHW 1.0; Firmware Version: SCOS 1.0 with Entrust IdentityGuard PIV Applet 1.0.1 Patch 172799

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1883	02/08/2013	eToken 5100, 5105, 5200 and 5205	SafeNet, Inc.	Hardware Versions: eToken 5100, eToken 5105, eToken 5200 and eToken 5205; Firmware Version: Athena IDProtect 0106.0113.2109 with SafeNet eToken Applet Suite 1.2.9
1884	02/08/2013	Totemo Cryptographic Module (TCM)	Totemo AG	Software Version: 2.0
1885	02/08/2013	3U VPX-1TB FSM Flash Storage Module	Curtiss-Wright Controls Defense Solutions	Hardware Versions: RHFS-3UR1024-F, RHFS-3UJ1024-F; Firmware Version: 1.11
1886	02/08/2013	DMD2050E TRANSEC Module	Comtech EF Data Corporation	Hardware Version: PL-0000192-1, Revision A; Firmware Version: 1.2.1
1887	02/08/2013	Cambium PTP 600 Series Point to Point Wireless Ethernet Bridges	Cambium Networks Ltd.	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 Versions: PTP600-10-00-FIPS and PTP600-10-05-FIPS
1888	02/11/2013	Cisco Aironet 1552E Outdoor Access Point	Cisco Systems, Inc.	Hardware Version: AIR-CAP1552E-A-K9 Revision: B0; FIPS Kit Version AIRLAP-FIPSKIT=; Firmware Versions: 7.0.116.0, 7.0.230.0 and 7.2.103.0
1889	02/13/2013	Wi-Q OMW (OW2000) [1], WAC (SDC2K) [2], WDC [3], and WXC [4] Controllers	Stanley Security Solutions, Inc.	Hardware Versions: 12681B [1]; 82065A [2]; 82069B [3]; 82069C [3]; 82069E [3]; 82069F [3] 82376C [4]; 82376D [4]; 82376F [4]; 82376G [4]; Firmware Version: 3.00.039

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1890	02/19/2013	SiteProtector Cryptographic Module	IBM Internet Security Systems, Inc.	Software Version: 1.1
1900	02/21/2013	Gemalto MultiApp ID V2.1	Gemalto	Hardware Versions: P5CC081 [1] and P5CC145 [2]; Firmware Version: MultiApp ID V2.1 with softmask V2.2 [1] and V2.4 [2] and Demonstration Applet V1.1 [1,2]
1901	02/21/2013	Red Hat Enterprise Linux 6.2 Kernel Crypto API Cryptographic Module	Red Hat®, Inc.	Software Version: 2.0
1902	02/21/2013	Imation S250/D250	Imation Corp.	Hardware Versions: D2-S250-S01, D2-S250-S02, D2-S250-S04, D2-S250-S08, D2-S250-S16, D2-S250-S32, D2-D250-B01, D2-D250-B02, D2-D250-B04, D2-D250-B08, D2-D250-B16, D2-D250-B32 and D2-D250-B64; Firmware Version: 4.5.0
1903	02/22/2013	Mocana Cryptographic Loadable Kernel Module	Mocana Corporation	Software Version: 5.5f