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

TM

Consolidated Certificate No. 0004

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: April 6, 2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: ____________________

Dated: March 31, 2011

Director, Industry Program Group
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
1493	03/21/2011	Sony Security Module	Sony Corporation	Hardware Version: 1.1.0; Firmware Version: 1.1.0
1494	03/21/2011	Sony Security Module	Sony Corporation	Hardware Version: 1.0.1; Firmware Version: 1.0.1
1495	02/28/2011			
1506	02/28/2011			
1507	03/02/2011	F-Secure Kernel Mode Cryptographic Driver	F-Secure Corporation	Software Version: 2.3.9
1509	03/02/2011	CodeXML® FIPS Bluetooth® Modem	Code Corporation	Hardware Version: P/N BTHDFIPS-M2_01; Firmware Version: 0187
1510	03/02/2011	F-Secure Kernel Mode Cryptographic Driver for Linux	F-Secure Corporation	Software Version: 2.3.9
1511	03/04/2011	NITROX XL 1600-NFBE HSM Family	Cavium Networks	Hardware Versions: P/Ns CN1620-NFBE1NIC-2.0-G, CN1620-NFBE2NIC-2.0-G, CN1620-NFBE3NIC-2.0-G, CN1610-NFBE1NIC-2.0-G, CN1620-NFBE1-2.0-G, CN1620-NFBE2-2.0-G, CN1620-NFBE3-2.0-G and CN1610-NFBE1-2.0-G, Version: 2.0; Firmware Version: 2.0
1512	03/04/2011	SafeNet Encryptor, Model 650	SafeNet, Inc.	Hardware Versions: 904-53260-007, 904-53261-007, 904-53361-20p, 943-53270-007, 943-53271-007 and 943-53371-20p; Firmware Version: 4.0.2
1513	03/04/2011	SafeNet Encryptor, Model 600	SafeNet, Inc.	Hardware Versions: 904-10001-00x, 904-10002-00x, 904-10003-00x, 904-10014-00x, 904-10112-00x, 904-10113-00x, 904-20001-00x, 904-20002-00x, 904-20003-00x, 904-25005-00x, 904-30013-00x, 904-511i0-00p, 904-511i1-00p, 943-511i0-00p and 943-511i1-00p; Firmware Version: 4.0.2

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1514	03/09/2011	Apple FIPS Cryptographic Module	Apple Inc.	Software Version: 1.0
1515	03/09/2011	Motorola PTP 600 Series	Motorola, 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; P/N WB3593 (HW Security Upgrade Kit); Firmware Version: PTP600 08-50
1516	03/11/2011	HP Enterprise Secure Key Manager	Hewlett-Packard Company	Hardware Version: P/N AJ575A, Version 2.1; Firmware Version: 4.8.9

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1517	03/11/2011	Aruba 3000 and 6000/M3 Mobility Controllers with ArubaOS Firmware	Aruba Networks, Inc.	Hardware Versions: 3200: 3200-8-AOS-STD-FIPS-US; 3400: 3400-32-AOS-STD-FIPS-US; 3600: 3600-64-AOS-STD-FIPS-US; 6000: (6000-BASE-2PSU-200-FIPS or 6000-BASE-2PSU-400-FIPS) with [(minimum one: LC-2G-1, LC-2G24F-1 or LC-2G24FP-1) and (one or two: M3mk1-G10X-10G2X)] (no more than four total); 3200 Revision C4: 3200-8-AOS-STD-FIPS-US Revision C4; 3400 Revision C4: 3400-32-AOS-STD-FIPS-US Revision C4; 3600 Revision C4: 3600-64-AOS-STD-FIPS-US Revision C4; 6000 Revision C4: (6000-BASE-2PSU-200-FIPS or 6000-BASE-2PSU-400-FIPS) with [(minimum one: LC-2G-1, LC-2G24F-1 or LC-2G24FP-1) and (one or two: M3mk1-G10X-10G2X Revision C4)] (no more than four total); Firmware Versions: 3200, 3400 and 3600: A3000_3.3.2.0-FIPS, A3000_3.3.2.11-FIPS, A3000_3.3.2.14-FIPS, A3000_3.3.2.18-FIPS, A3000_3.3.2.19-FIPS, A3000_3.3.2.20-FIPS or A3000_3.4.2.3-FIPS; 6000: ArubaOS_MMC_3.3.2.0-FIPS, ArubaOS_MMC_3.3.2.11-FIPS, ArubaOS_MMC_3.3.2.14-FIPS, ArubaOS_MMC_3.3.2.18-FIPS, ArubaOS_MMC_3.3.2.19-FIPS, ArubaOS_MMC_3.3.2.20-FIPS or ArubaOS_MMC_3.4.2.3-FIPS
1518	03/11/2011	IMB	GDC Technology (USA), LLC	Hardware Version: GDC-IMB-v1; Firmware Version: 1.1

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1519	03/11/2011	Code Reader 2500 FIPS and Code Reader 3500 FIPS	Code Corporation	Hardware Versions: P/Ns 2512FIPS_01 and 3512FIPS_01; Firmware Version: 4641
1520	03/11/2011	Cisco 1905, Cisco 1921, Cisco 1941, Cisco 2901, Cisco 2911 and Cisco 2921 Integrated Services Routers (ISRs)	Cisco Systems, Inc.	Hardware Version: 1905 [1][2], 1921 [1][2], 1941 [1][2], 2901 [1][3], 2911 [1][4], 2921 [1][5], FIPS Kit (CISCO-FIPS-KIT=), Revision -B0 [1], ISR: FIPS-SHIELD-1900= [2], FIPS-SHIELD-2901= [3], FIPS-SHIELD-2911= [4] and FIPS-SHIELD-2921= [5]; Firmware Version: 15.1(2)T2A
1521	03/18/2011	Cisco 2951, Cisco 3925 and Cisco 3945 Integrated Services Routers (ISRs)	Cisco Systems, Inc.	Hardware Versions: 2951 [1][2], 3925 [1][3], 3945 [1][3], FIPS Kit (CISCO-FIPS-KIT=), Revision -B0 [1], ISR: FIPS-SHIELD-2951= [2] and FIPS-SHIELD-3900= [3]; Firmware Version: 15.1(2)T2A
1522	3/23/2011	IBM LTO Generation 5 Encrypting Tape Drive	IBM® Corporation	Hardware Versions: 45E8192 EC Level M11221 (Fibre Channel) and 45E8193 EC Level M11221 (SAS); Firmware Versions: pf100923e.A9Q5.FC.fips.ro (Fibre Channel) and pf100923e.A9Q5.SAS.fips.ro (SAS)
1524	03/23/2011	SafeNet Luna EFT	SafeNet, Inc.	Hardware Version: GRK-09-0100; Firmware Version: MAL00000E
1526	03/24/2011	Lexmark PrintCryption™	Lexmark International Inc.	Firmware Version: 1.3.2f