FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0031

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: Don FD
Dated: 8 August 2013

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: D.J. Mc
Dated: 6 August 2013
for:
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
1970	07/02/2013	iStorage FIPS Module 140-2	iStorage Limited	Hardware Version: REV. A; Firmware Version: 4.0
1971	07/03/2013	3e-520 Secure Access Point Cryptographic Module	3e Technologies International, Inc.	Hardware Version: 1.0; Firmware Version: 5.0
1972	07/05/2013	HiPKI SafGuard 1200 HSM	Chunghwa Telecom Laboratories	Hardware Version: HSM-HW-20; Firmware Version: HSM-SW-20
1973	07/10/2013	McAfee Firewall Enterprise Virtual Appliance for Crossbeam XOS	McAfee, Inc.	Software Version: 8.2.1
1975	07/17/2013	Accellion Cryptographic Module	Accellion, Inc.	Software Version: FTALIB_2_0_1
1976	07/17/2013	VSX	Check Point Software Technologies, Ltd.	Firmware Version: R67.10 with R7x hotfix
1977	07/17/2013	Security Gateway	Check Point Software Technologies, Ltd.	Firmware Version: R70.1 with R7x hotfix
1978	07/17/2013	Security Management	Check Point Software Technologies, Ltd.	Firmware Version: R71 with R7x hotfix
1979	07/17/2013	Provider-1	Check Point Software Technologies, Ltd.	Firmware Version: R71 with R7x hotfix
1980	07/17/2013	Cocoon Data Secure Objects C++ Cryptographic Module Version 1.8	Cocoon Data Holdings Limited	Software Version: 1.8
1981	07/17/2013	Kanguru Defender 2000™ Cryptographic Module	Kanguru Solutions	Hardware Versions: P/Ns KVD-SMCF-32G, KVD-SMCF-16G, KDF2000-32G, KDF2000-64G, KDF2000-128G, KDF2000-16G, KDF2000-8G, KDF2000-4G, KDF2000-S16G, KDF2000-S2G, KDF2000-S4G and KDF2000-S8G, Version 1.0; Firmware Version: 2.03.10

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1982	07/17/2013	Cisco Catalyst 4503-E, Catalyst 4506-E, Catalyst 4507R-E, Catalyst 4507R+E, Catalyst 4510R-E, Catalyst 4510R+E with Supervisor Cards (WS-X45-SUP7-E and WS-X45-Sup7L-E) and Line Cards (WS-X4748-RJ45V+E, WS-X4712-SFP+E, WS-X4640-CSFP-E, WS-X4748-NGPOE+E, and WS-X4748-RJ45-E)	Cisco Systems, Inc.	Hardware Versions: Catalyst 4503-E [1, 3, 4, 5, 6, A], Catalyst 4503-E [2, 5, 7, A], Catalyst 4506-E [1, 3, 4, 5, 6, 7, B], Catalyst 4506-E [2, 3, 4, 5, 6, 7, B], Catalyst 4507R-E [1, 3, 4, 5, 6, 7, C], Catalyst 4507R-E [2, 3, 4, 5, 6, 7, C], Catalyst 4507R+E [1, 3, 4, 5, 6, 7, C], Catalyst 4507R+E [2, 3, 4, 5, 6, 7, C], Catalyst 4510R-E [1, 3, 4, 5, 6, 7, D], Catalyst 4510R+E [1, 3, 4, 5, 6, 7, D], Supervisor Card WS-X45-SUP7-E [1], Supervisor Card WS-X45-SUP7L-E [2], Line Card WS-X4748-RJ45V+E [3], Line Card WS-X4712-SFP+E [4], Line Card WS-X4640-CSFP-E [5], Line Card WS-X4748-NGPOE+E [6], Line Card WS-X4748-RJ45-E [7], FIPS kit packaging (WS-C4503-FIPS-KIT= [A], WS-C4506-FIPS-KIT= [B], WS-C4507-FIPS-KIT= [C] and WS-C4510-FIPS-KIT= [D]) and Filler Plate (C4K-SLOT-CVR-E); Firmware Version: 3.3.1SG
1983	07/23/2013	AX Series Advanced Traffic Manager AX2500, AX2600-GCF, AX3000-11-GCF, AX5100, AX5200-11, AX1030, AX3030, AX3400, AX3200-12, AX3530 and AX5630	A10 Networks, Inc.	Hardware Versions: AX2500[1,2], AX2600-GCF[1,2], AX3000-11-GCF[1,2], AX5100[1,2], AX5200-11[1,2], AX1030[2], AX3030[2], AX3400[2], AX3200-12[2], AX3530[2] and AX5630[2]; Firmware Versions: R261-GR1-P7[1] and R270-P2[2]
1984	07/23/2013	eToken	SafeNet, Inc.	Hardware Version: Inside Secure AT90SC25672RCT-USB; Firmware Version: Athena IDProtect 0106.0113.2109 with SafeNet eToken Applet Suite 1.2.9
1985	07/23/2013	Samsung FIPS BC for Mobile Phone and Tablet	Samsung Electronics Co., Ltd.	Software Version: SBC1.45_1.1