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. 0029

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: 5 June 2013

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: ______________________

Dated: 4 June 2013

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
1917	05/21/2013	Brocade® MLXe® and Brocade NetIron® CER Series Ethernet Routers	Brocade Communications Systems, Inc.	Hardware Versions: BR-MLXE-4-MR-M-AC, BR-MLXE-4-MR-M-DC, BR-MLXE-8-MR-M-AC, BR-MLXE-8-MR-M-DC, BR-MLXE-16-MR-M-AC, BR-MLXE-16-MR-M-DC, NI-CER-2024C-ADVPREM-AC, NI-CER-2024C-ADVPREM-DC, NI-CER-2024F-ADVPREM-AC, NI-CER-2024F-ADVPREM-DC, NI-CER-2048FX-ADVPREM-AC, NI-CER-2048FX-ADVPREM-DC, NI-CER-2048F-ADVPREM-AC, NI-CER-2048F-ADVPREM-DC, NI-CER-2048C-ADVPREM-AC, NI-CER-2048C-ADVPREM-DC, NI-CER-2048CX-ADVPREM-AC and NI-CER-2048CX-ADVPREM-DC with FIPS Kit (P/N Brocade XBR-000195) and NI-MLX-MR Management Module; Firmware Version: IronWare Software R05.1.01a
1942	05/02/2013	Cisco Catalyst C4500X-32SFP+ and Catalyst C4500X-F-32SFP+	Cisco Systems, Inc.	Hardware Versions: Catalyst C4500X-32SFP+ and Catalyst C4500X-F-32SFP+; FIPS kit packaging (CVPN4500FIPS/KIT=); Firmware Version: 3.3.1SG
1943	05/02/2013	Evolution e8350™ - Satellite Router [1], iConnex e800™ - Satellite Router Board [2], iConnex e850MP™ Satellite Router Board [3], iConnex e850MP™ - IND Satellite Router Board [4], iConnex e850MP™ - IND with Heat Sink Satellite Router Board [5], Evolution eM1D1™ Line Card [6] and Evolution eM0DM™	VT iDirect, Inc.	Hardware Versions: Part #E0000051-0003 [1]; Part #E0001340-0002 [2]; Part #E0000731-0001 [3]; E0000731-0002 [4]; Part #E0000731-0003 [5]; Part #E0000080-0002 [6]; Part #E0000080-0005 [7]; Firmware Version: iDX version 2.3.1
1944	05/03/2013	Apple iOS CoreCrypto Kernel Module, v3.0	Apple Inc.	Software Version: 3.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1946	05/14/2013	TW-400 (CUB)	TrellisWare Technologies Inc.	Hardware Version: ASY0540250 rev X1; Firmware Version: 4c-beta2-FIPS
1947	05/16/2013	TW-230 (CheetahNet II)	TrellisWare Technologies Inc.	Hardware Version: ASY0560001 rev X2; Firmware Version: 4c-beta2-FIPS
1948	05/16/2013	Samsung OpenSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: SFOpenSSL1.0.0e-1.1
1949	05/16/2013	Harris AES Software Load Module	Harris Corporation	Software Version: R04A01
1950	05/23/2013	FortiGate-1000C [1], FortiGate-1240B [2] and FortiGate-3140B [3]	Fortinet, Inc.	Hardware Versions: C4HR40 [1], C4CN43 [2] and C4XC55 [3] with Tamper Evident Seal Kits: FIPS-SEAL-RED [1,3] or FIPS-SEAL-BLUE [2]; Firmware Version: FortiOS 4.0, build 8963, 121031
1951	05/23/2013	FortiGate-80C [1], FortiGate-110C [2], FortiGate-60C [3] and FortiWiFi-60C [4]	Fortinet, Inc.	Hardware Versions: C4BC61 [1], C4HA15 [2], C4DM93 [3] and C4DM95 [4] with Tamper Evident Seal Kits: FIPS-SEAL-BLUE [1,2] or FIPS-SEAL-RED [3,4]; Firmware Version: FortiOS 4.0, build 8963, 121031
1952	05/23/2013	3S Group Cryptographic Module (3SGX)	3S Group Incorporated	Hardware Version: 1.0; Firmware Version: 1.0
1953	05/23/2013	NXP JCOP 2.4.2 R2	NXP Semiconductors	Hardware Versions: P5CC081 V1A, P5CD081 V1A, P5CD081 V1D, P5CC145 V0B and P5CD145 V0B; Firmware Versions: JCOP 2.4.2 R2 Mask ID 59 and patchID 3 with Demonstration Applet v1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1954	05/30/2013	Enhanced Bandwidth Efficient Modem (EBEM) Cryptographic Module	ViaSat, Inc.	Hardware Versions: P/Ns 1010162 Version 1, 1010162 with ESEM Version 1, 1091549 Version 1, 1075559 Version 1, 1075559 with ESEM Version 1, 1091551 Version 1, 1010163 Version 1, 1010163 with ESEM Version 1, 1091550 Version 1, 1075560 Version 1, 1075560 with ESEM Version 1 and 1091552 Version 1; Firmware Version: 02.03.02