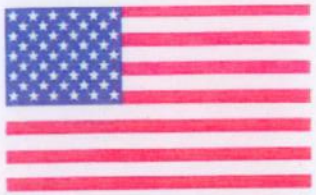
FIPS 140-2 Consolidated Validation Certificate



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. 0028

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: Dan FD

Dated: 06 May 2013

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 3 May 2013

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1925	04/04/2013	Samsung Key Management Module	Samsung Electronics Co., Ltd.	Software Version: KM1.1
1927	04/08/2013	FEITIAN-FIPS-COS	Feitian Technologies Co., Ltd.	Hardware Version: 1.0.0; Firmware Version: 1.0.0
1928	04/08/2013	Christie IMB-S2 4K Integrated Media Block (IMB)	Christie Digital Systems Canada, Inc.	Hardware Version: 000-102675-01; Firmware Versions: 1.0.1-2641 or 1.0.3-3047 or 1.1.0-3271 or 1.2.0-3400 or 1.2.1-3546
1929	04/08/2013	SRA EX9000	SonicWALL, Inc.	Hardware Version: P/N 101-500352-50 Rev A; Firmware Version: SRA 10.6.1
1930	04/08/2013	OpenSSL Module	SUSE Linux Products GmbH	Software Version: 0.9.8j
1931	04/08/2013	SafeZone FIPS Cryptographic Module	INSIDE Secure	Software Version: 1.0.3
1932	04/08/2013	Cisco ASA 5505, ASA 5510, ASA 5520, ASA 5540, ASA 5550, ASA 5580-20, ASA 5580-40, ASA 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40 and 5585-X SSP-60 Security Appliances	Cisco Systems, Inc.	Hardware Versions: 5505 [1, 2], 5510 [1], 5520 [1], 5540 [1], 5550 [1], 5580-20 [3], 5580-40 [3], 5585-X SSP-10 [4], 5585-X SSP-20 [4], 5585-X SSP-40 [4], 5585-X SSP-60 [4] with [FIPS Kit (DS-FIPS-KIT= Rev -BO)] [1], [ASA 5505 FIPS Kit (ASA5505-FIPS-KIT Rev-A0)] [2], [ASA 5580 FIPS Kit (ASA5580-FIPS-KIT)] [3] or [ASA 5585 FIPS Kit (ASA5585-X-FIPS-KIT)] [4]; Firmware Version: 8.4.4.1
1933	04/15/2013	Red Hat Enterprise Linux 6.2 dm-crypt Cryptographic Module	Red Hat®, Inc.	Software Version: 2.0
1934	04/18/2013	Evolution e8350™ - FIPSL2 Satellite Router [1], iConnex e800™ - FIPSL2 Satellite Router Board [2], iConnex e850MP™ - FIPSL2 Satellite Router Board [3], Evolution eM1D1™ - FIPSL2 Line Card [4] and Evolution eM0DM™ - FIPSL2 Line Card [5]	VT iDirect, Inc.	Hardware Versions: Part #E0000051-0005 [1]; Part #E0001340-0001 [2]; Part #E0000731-0004 [3]; Part #E0001306-0001 [4]; Part #E0001306-0002 [5]; Firmware Version: iDX version 2.3.1

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1935	04/18/2013	Cisco 5915 Embedded Services Routers	Cisco Systems, Inc.	Hardware Versions: Cisco 5915 ESR air-cooled card and Cisco 5915 ESR conduction-cooled card; Firmware Version: 1.0
1936	04/24/2013	Mxtran Payeeton Solution	Mxtran Inc.	Hardware Version: MX12E320128E; Firmware Version: Simker v3.20
1937	04/30/2013	Symantec App Center Cryptographic Module	Symantec Corporation	Software Version: 1.0
1938	04/30/2013	CryptoComply™ | Mobile	SafeLogic, Inc.	Software Version: 2.1
1939	04/30/2013	HiCOS PKI Native Smart Card	Chunghwa Telecom Co., Ltd.	Hardware Versions: HD65255C1 and HD65257C1; Firmware Versions: HardMask: 2.1 and SoftMask: 1.0
1940	04/30/2013	IOS Common Cryptographic Module (IC2M)	Cisco Systems, Inc.	Firmware Versions: Rel 1(1.0.0), Rel 1(1.0.1) and Rel 1(1.0.2)
1941	04/30/2013	Proventia GX Series Security Appliances	IBM Internet Security Systems, Inc.	Hardware Versions: GX7800 and GX7412; with FIPS-LABELS: FIPS 140 tamper evidence labels; Firmware Version: 4.3