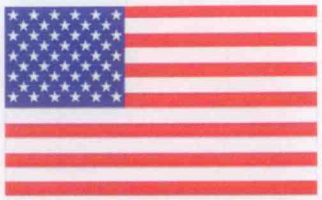
FIPS 140-2 Consolidated Validation Certificate



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. 0046

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 A Cooper

Dated: 11/12/2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 6 November 2014

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2239	10/16/2014	McAfee Core Cryptographic Module (user)	McAfee, Inc.	Software Version: 1.0
2261	10/01/2014	Cryptographic Module for CipherCloud Gateway	CipherCloud, Inc.	Software Version: 1.0
2262	10/01/2014	Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model)	Toshiba Corporation	Hardware Versions: A0 with PX02SMU020, PX02SMU040, PX02SMU080 or PX02SMQ160; Firmware Version: NA00
2263	10/07/2014	SafeGuard® CryptoServer Se	Utimaco IS GmbH	Hardware Version: P/N CryptoServer Se, Version 3.00.3.1; Firmware Version: 3.0.1.0
2264	10/10/2014	HGST Ultrastar C15K600 TCG Enterprise HDDs	HGST, Inc.	Hardware Versions: HUC156060CS4205 [1], HUC156045CS4205 [1], HUC156030CS4205 [1], HUC156060CSS205 [1], HUC156045CSS205 [1] and HUC156030CSS205 [1]; Firmware Version: R3A0
2265	10/10/2014	HealthStackIO Platform Cryptographic Module	HealthStackIO Inc.	Software Version: 1.0
2266	10/10/2014	CHN-II	Digicine Oristar Technology Development (Beijing) Co., Ltd	Hardware Version: 1.0; Firmware Version: 1.0.0, Bootloader Version:1.0
2267	10/14/2014	Yubico YubiKey Standard and YubiKey Nano	Yubico Inc.	Hardware Version: 1.6; Firmware Version: 2.5.1
2268	10/16/2014	Globo Plc Mobile Cryptographic Module	Globo Plc	Software Version: 1.0
2269	10/16/2014	Globo Plc Server Cryptographic Module	Globo Plc	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2270	10/22/2014	Cisco Optical Networking Solution (ONS) 15454 Multiservice Transport Platforms (MSTPs)	Cisco Systems, Inc.	Hardware Versions: [15454-M2-SA, 15454-M6-SA, 15454-M-TNC-K9, 15454-M-TSC-K9, 15454-M-TNCE-K9, 15454-M-TSCE-K9, 15454-M-WSE-K9 and 10X10G-LC] with FIPS Kit: CISCO-FIPS-KIT=; Firmware Version: 9.8.1.2
2271	10/24/2014	AQ42-M	Digicine Oristar Technology Development (Beijing) Co., Ltd.	Hardware Version: 2.0.0; Firmware Version: 1.2.2
2272	10/24/2014	VaultIP	INSIDE Secure	Hardware Version: 1.1.4; Firmware Version: 1.1.4