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. 0038

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 J Cooper

Dated: 3/21/2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 13 Mar '14

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2074	02/22/2014	Embeddable Security System (ES-1200)	ViaSat, Inc.	Hardware Version: P/N 1174941, Rev. 001; Firmware Version: 1.0.7
2076	02/06/2014	Oracle Solaris Userland Cryptographic Framework with SPARC T4 and SPARC T5	Oracle Corporation	Hardware Versions: 527-1437-01 and 7043165; Software Versions: 1.0 and 1.1
2077	02/06/2014	Oracle Solaris Userland Cryptographic Framework	Oracle Corporation	Software Versions: 1.0 and 1.1
2078	02/06/2014	CAT904 Dolby® JPEG 2000/MPEG-2 Processor	Dolby Laboratories, Inc.	Hardware Versions: P/N CAT904Z Revisions FIPS_1.0, FIPS_1.0.1, FIPS_1.0.2 and FIPS_1.1; Firmware Version: 1.3.4.21
2079	02/07/2014	HP-UX Kernel Cryptographic Module	Hewlett Packard Development Company, L.P.	Software Version: 1.0
2080	02/10/2014	CN6000 Series Encryptors	Senetas Corporation Ltd. and SafeNet Inc.	Hardware Versions: CN6040 Series: A6040B [O] (AC), A6040B [Y] (AC), A6041B [O] (DC), A6041B [Y] (DC), A6042B [O] (AC/DC) and A6042B [Y] (AC/DC); CN6100 Series: A6100B [O] (AC), A6100B [Y] (AC), A6101B [O] (DC), A6101B [Y] (DC), A6102B [O] (AC/DC) and A6102B [Y] (AC/DC); Firmware Version: 2.3.0
2081	02/22/2014	V2VNet Common Crypto Module	Dispersive Solutions, Inc.	Software Version: 1.0
2082	02/13/2014	Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)	Toshiba Corporation	Hardware Version: AA; Firmware Version: FN001S
2083	02/22/2014	TS-250	FiberLogic Communications, Inc.	Hardware Version: 1.0; Firmware Version: 1.0.0.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2084	02/22/2014	GO-Trust SDencrypter	GOTrust Technology Inc.	Hardware Versions: GT-3001 with GT-0330; Firmware Versions: 4.1.0.8 with 80023802-33860406 and 80023802-33860506
2085	02/22/2014	VPX3-685 Secure Routers	Curtiss-Wright Controls Defense Solutions	Hardware Versions: Air-Cooled Chassis: VPX3-685-A13014-FC and VPX3-685-A13020-FC; Conduction-Cooled Chassis: VPX3-685-C23014-FC and VPX3-685-C23020-FC; Firmware Version: 2.0
2086	02/22/2014	StorageTek T10000C Tape Drive	Oracle Corporation	Hardware Version: P/N 7054185; Firmware Version: 1.57.308
2087	02/24/2014	Server Crypto Module	Fixmo Inc.	Software Version: 1.0
2088	02/25/2014	McAfee Database Security Sensor Cryptographic Module	McAfee, Inc.	Software Version: 1.0
2089	02/25/2014	HGST Ultrastar SSD800/1000 TCG Enterprise SSDs	HGST, Inc.	Hardware Versions: P/Ns HUSMH8080ASS205 [0001], HUSMH8040ASS205 [0001], HUSMH8020ASS205 [0001], HUSMM8080ASS205 [0001], HUSMM8040ASS205 [0001], HUSMM8020ASS205 [0001], HUSMR1010ASS205 [0001], HUSMR1050ASS205 [0001] and HUSMR1025ASS205 [0001]; Firmware Version: R190

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2090	02/26/2014	Cisco ASR 1001 [1][K1], ASR 1002 [2][K2][E1 or E2], ASR1002-X [3][K2], ASR 1004 [4][K3][R1 or R2][E2, E3 or E4], ASR 1006 [5][K4][single or dual E2, E3, E4 or E5][dual R1 or R2] and ASR 1013 [6][K5][E4 or E5][R2]	Cisco Systems, Inc.	Hardware Versions: ASR1001 [1], ASR1002 [2], ASR1002-X [3], ASR1004 [4], ASR1006 [5] and ASR1013 [6]; FIPS KITs: ASR1001-FIPS-Kit [K1], ASR1002- FIPS-Kit [K2], ASR1004-FIPS-Kit [K3], ASR1006-FIPS-Kit [K4] and ASR1013-FIPS-Kit [K5]; Embedded Services Processors: ASR1000-ESP5 [E1], ASR1000-ESP10 [E2], ASR1000-ESP20 [E3], ASR1000-ESP40 [E4] and ASR1000-ESP100 [E5]; Route Processors: ASR-1000-RP1 [R1] and ASR-1000-RP2 [R2]; Firmware Version: 3.7.2tS
2091	02/26/2014	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 and 15454-M-WSE-K9] with FIPS Kit: CISCO-FIPS-KIT=; Firmware Version: 9.8
2092	02/26/2014	Samsung FIPS BC for Mobile Phone and Tablet	Samsung Electronics Co., Ltd.	Software Versions: SBC1.45_2.0 and SBC1.45_2.1
2093	02/27/2014	Cisco Catalyst 3560-C [1], 3560-X [2] and 3750-X [3] Switches	Cisco Systems, Inc.	Hardware Versions: [3560CG-8PC-S, 3560CG-8TC-S and 3560CPD-8PT-S] [1] [B], [(WS-C3560X-24P-L and WS-C3560X-48T-L) [2] and (WS- C3750X-12S, WS-C3750X-24S, WS-C3750X-24T, WS-C3750X-48P and WS-C3750X-48T) [3]] with [C3KX-SM-10G, C3KX-NM-1G, C3KX-NM-10G, C3KX-NM-BLANK and C3KX-NM-10GT] [A] with FIPS kit packaging [C3KX-FIPS-KIT 700-34443-01] [A] and [C3KX-FIPS-KIT 47-25129-01] [B]; Firmware Version: 15.0(2)SE3
2094	02/28/2014	Intelligence Platform Cryptographic Module	Securonix, Inc.	Software Version: 1.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2095	02/28/2014	App Center Server Cryptographic Module	Symantec Corporation	Software Version: 1.0