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

October 2017

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, 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: 11/2/2017

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: NOV 2 | 17

Director, Architecture and Technology Assurance
Communications Security Establishment

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

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
3033	10/02/2017	Titan Key	Google, Inc.	Hardware Version: 1.0; Firmware Version: 1.0
3034	10/02/2017	Blue Coat ProxySG S400-20 [1], S400-30 [2], S400-40 [3], S500-10 [4], S500-20 [5] and S500-30 [6]	Symantec Corporation	Hardware Version: 090-03075 [1], 090-03076 [1], 090-03079 [2], 090-03080 [2], 090-03083 [3], 090-03084 [3], 090-02998 [4], 090-02999 [4], 090-03000 [5], 090-03001 [5], 090-03579 [6] and 090-03580 [6] with FIPS Kit: HW-KIT-FIPS-400 [1,2,3] and HW-KIT-FIPS-500 [4,5,6]; Firmware Version: 6.7.2
3035	10/03/2017	nShield Solo XC F3 [1] and nShield Solo XC F3 for nShield Connect XC [2]	Thales e-Security Inc.	Hardware Version: NC4035E-000 [1] and NC4335N-000 [2], Build Standard A; Firmware Version: 3.3.21
3036	10/04/2017	Huawei USG 6000 Series Firewall	Huawei Technologies Co., Ltd.	Hardware Version: USG6310S (P/N 50050064 Rev. G), USG6370 (P/N 0235G7LL Rev. P.4), USG6620 (P/N 02359519 Rev. G.3), USG6650 (P/N 0235G7G4 Rev. U.3) and USG6680 (P/N 0235G7G7 Rev. U.2); External Baffle: 99089JEB, Version A.2; Tamper Seal 4057-113016, Version A.3; Firmware Version: V500R001C50
3037	10/04/2017	Symantec Advanced Secure Gateway S400-20 [1], S400-30 [2], S400-40 [3], S500-10 [4] and S500-20 [5]	Symantec Corporation	Hardware Version: 090-03513 [1], 090-03516 [2], 090-03520 [3], 090-03527 [4] and 090-03531 [5] with FIPS Kit: HW-KIT-FIPS-400 [1,2,3] and HW-KIT-FIPS-500 [4,5]; Firmware Version: 6.7.2
3038	10/05/2017	SUSE Linux Enterprise Server OpenSSL Module	SUSE, LLC	Software Version: 3.0
3039	10/06/2017	ID-One PIV on Cosmo V8.1 - SPE Configurations	Oberthur Technologies	Hardware Version: P/Ns '30-5F01' [1] and '40-6001' [2]; Firmware Version: Firmware Extensions: '086294'+'086683' (ID-One PIV Applet Suite 2.4.0 on Cosmo V8.1 LARGE) [1] and Firmware Extension: '086294'+'086693' (ID-One PIV Applet Suite 2.4.0 on Cosmo V8.1 STD) [2]
3040	10/10/2017	nShield Solo XC F2	Thales e-Security Inc.	Hardware Version: NC3025E-000; Firmware Version: 3.3.21
3041	10/11/2017	Datacryptor(R) Gig Ethernet and 10 Gig Ethernet	Thales e-Security Inc.	Hardware Version: 1600x433, Rev. 01, Rev. 02 and 1600x437, Rev. 01, Rev. 02; Firmware Version: 5.0 and 5.1
3042	10/11/2017	Datacryptor(R) 100M Ethernet	Thales e-Security Inc.	Hardware Version: 1600x439, Rev. 01 and 1600x439, Rev. 02; Firmware Version: 5.0 and 5.1
3043	10/13/2017	CA Technologies C-Security Kernel	CA, Inc. dba CA Technologies	Software Version: 3.11.2
3046	10/17/2017	Distech Java Cryptographic Module	Distech Controls Inc.	Firmware Version: 1.0
3047	10/17/2017	Xirrus XR Series Wi-Fi Products	Xirrus, Inc.	Hardware Version: P/Ns XR-630-FIPS, XR-2436, XR-4836; XE-6000-TBAR (Enclosure Form Factor); SKU XE-LABEL-FIPS (Tamper-Evident Seals); Firmware Version: AOS-8.2
3048	10/17/2017	Reverse Proxy S400-20 [1], S400-30 [2], S400-40 [3], S500-10 [4], S500-20 [5] and S500-30 [6]	Symantec Corporation	Hardware Version: 090-03623 [1], 090-03626 [1], 090-03624 [2], 090-03627 [2], 090-03625 [3], 090-03628 [3], 090-03615 [4], 090-03617 [4], 090-03616 [5], 090-03618 [5], 090-03656 [6] and 090-03657 [6] with FIPS Kit: HW-KIT-FIPS-400 [1,2,3] and HW-KIT-FIPS-500 [4,5,6]; Firmware Version: 6.7.2

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
3049	10/17/2017	CN8000 Multi-slot Encryptor	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet) and ID Quantique SA	Hardware Version: A8003-01, A8003-02, A8003-03, A8003-04, A8003-05, A8003-06, A8003-07, A8003-08, A8003-09 and A8003-10; Firmware Version: 3.0.1
3050	10/17/2017	CN6000 Series Encryptors	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN6040 Series: A6040B (AC), A6041B (DC) and A6042B (AC/DC); Senetas Corp. Ltd. CN6100 Series: A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN6040 Series: A6040B (AC), A6041B (DC) and A6042B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN6100 Series: A6100B (AC), A6101B (DC) and A6102B (AC/DC); Firmware Version: 3.0.1
3051	10/18/2017	CN9000 Series Encryptors	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC); Senetas Corp. Ltd. CN9000 Series: A9120B (AC), A9121B (DC), A9122B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN9000 Series: A9120B (AC), A9121B (DC), A9122B (AC/DC); Firmware Version: 3.0.1
3052	10/19/2017	Samsung SAS 12G TCG Enterprise SSC SEDs PM1633a LC Series	Samsung Electronics Co., Ltd.	Hardware Version: MZILS3T8HMLH-000H9, MZILS1T9HEJH-000H9 and MZILS920HEHP-000H9; Firmware Version: 3P00
3053	10/19/2017	CN Series Ethernet Encryptors	Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN4000 Series: A4010B (DC), A4020B (DC); Senetas Corp. Ltd. CN6010 Series: A6010B (AC), A6011B (DC) and A6012B (AC/DC); Senetas Corp. Ltd. CN6140 Series: A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN4000 Series: A4010B (DC), A4020B (DC); Senetas Corp. Ltd. & SafeNet Inc. CN6010 Series: A6010B (AC), A6011B (DC) and A6012B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN6140 Series: A6140B (AC), A6141B (DC) and A6142B (AC/DC); Firmware Version: 3.0.1
3054	10/27/2017	CryptoSSC	SPAWAR Systems Center Pacific	Software Version: 1.0
3055	10/27/2017	Saviynt Cryptographic Module	Saviynt	Software Version: 1.0