globalscape
securely connected

Globalscape® EFT™ FIPS Certification

In 2008, Globalscape released a FIPS-certified cryptographic module. The GlobalSCAPE® Cryptographic Module (GSCM) provided cryptographic services for our managed file transfer product, EFT. The services included symmetric/asymmetric encryption/decryption, digital signatures, message digest, message authentication, random number generation, and SSL/TLS support. The GSCM was intended for use by applications through the module's Application Programming Interface (API), which is based on the OpenSSL API defined by the OpenSSL Project.

The GSCM was certified for:

- Meeting Level 1 with Microsoft Windows Server 2003 (single-user mode)
- FIPS Approved algorithms: AES (Cert. #618); Triple-DES (Cert. #586); DSA (Cert. #240); SHS (Cert. #666); RSA (Cert. #287); HMAC (Cert. #320); RNG (Cert. #388)
- Other algorithms: RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength); Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength); DES; MD2; MD4; MD5; MDC2; RIPEMD160; Blowfish; CAST5; RC2; RC4; RC5; IDEA

On November 15, 2015, NIST special publication 800-131A deprecated the random number generator, ANSI X9.62, used in that original FIPS-Certified library in the GSCM. As a result, the original Globalscape FIPS library could no longer be considered FIPS certified as of January 1, 2016. Therefore, Globalscape has deployed a new cryptographic library that has the proper updates and has attained FIPS certification.

What We Have Now

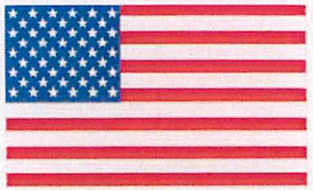
For the FIPS implementation in EFT version 7.2.9 and 7.3.6 (and subsequent releases), Globalscape is using version 2.0.10 of the OpenSSL FIPS Object Module.

Our development team, fulfilling the Crypto Officer role, built that library, and our EFT Server initializes that library in FIPS mode, according to its published security policy. As a result, our use of the library's cryptographic operations is compliant with the FIPS certification. Thus, although the certificate itself has changed (because we swapped out the older cryptographic library for a newer, safer one), the EFT Server itself is back to its former state of offering FIPS-certified cryptographic operations.

The NIST FIPS certificate is #1747, which can be found here:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747

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. 0018

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: 16 July, 2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 4 July 2012

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
1728	06/01/2012	Cisco Catalyst 6506, 6506-E, 6509 and 6509-E Switches with Wireless Services Modules-2 (WiSM2)	Cisco Systems, Inc.	Hardware Versions: Chassis: Catalyst 6506 switch [1], Catalyst 6506-E switch [2], Catalyst 6509 switch [3] and Catalyst 6509-E switch [4]; Backplane: WS-C6506 [1], WS-C6506-E [2], WS-C6509 [3] and WS-C6509-E [4]; FIPS Kit: P/N 800-27009 [1, 2], P/N 800-26335 [3, 4] and WS-SVCWISM2FIPKIT= [1, 2, 3, 4]; with one Supervisor Blade [1, 2, 3, 4]: [WS-SUP720-3BXL , WS-SUP720-3B, VS-S 720 10G-3C, or VS-S 720 10G-3CXL] and with one WiSM2 [1, 2, 3, 4]: [WS-SVC-WISM2-K9=, WS-SVC-WISM2-5-K9=, WS-SVC-WISM2-3-K9=, WS-SVC-WISM2-1-K9=, WS-SVC-WISM2-5-K9, WS-SVC-WISM2-3-K9 or WS-SVC-WISM2-1-K9]; Firmware Versions: [1, 2, 3, 4]: Supervisor Blade: Cisco IOS Release 12.2.33.SXJ; WiSM2: 7.0.116.0
1729	06/08/2012	Security Builder® FIPS Module	Certicom Corp.	Software Version: 6.0
1730	06/12/2012	Juniper Networks SSG 520M and SSG 550M	Juniper Networks, Inc.	Hardware Versions: [SSG-520M-SH, SSG-520M-SH-N, SSG-520M-SH-DC-N, SSG-520M-N-TAA, SSG-520M-SH-DC-N-TAA, SSG-550M-SH, SSG-550M-SH-N, SSG-550M-SH-DC-N, SSG-550M-N-TAA and SSG-550M-SH-DC-N-TAA] with JNPR-FIPS-TAMPER-LBLS; Firmware Version: ScreenOS 6.3r6

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1731	06/12/2012	SSG 320M and SSG 350M	Juniper Networks, Inc.	Hardware Versions: [SSG-320M-SB, SSG-320M-SH, SSG-320M-SB-TAA, SSG-320M-SH-TAA, SSG-320M-SB-DC-N-TAA, SSG-320M-SH-DC-N-TAA, SSG-350M-SB, SSG-350M-SH, SSG-350M-SB-TAA, SSG-350M-SH-TAA, SSG-350M-SB-DC-N-TAA and SSG-350M-SH-DC-N-TAA] with JNPR-FIPS-TAMPER-LBLS; Firmware Version: ScreenOS 6.3r6
1732	06/20/2012	Symantec Enterprise Vault Cryptographic Module	Symantec Corporation	Software Version: 1.0.0.2
1733	06/20/2012	nShield F3 6000e [1], nShield F3 1500e [2], nShield F3 500e [3], nShield F3 10e [4], nShield F3 6000e for nShield Connect [5], nShield F3 1500e for nShield Connect [6] and nShield F3 500e for nShield Connect [7]	Thales-eSecurity Inc.	Hardware Versions: nC4033E-6K0 [1], nC4033E-1K5 [2], nC4033E-500 [3], nC4033E-030 [4], nC4033E-6K0N [5], nC4033E-1K5N [6] and nC4033E-500N [7], Build Standard N; Firmware Version: 2.50.16-2
1734	06/21/2012	Imation S250/D250	Imation Corp.	Hardware Versions: D2-S250-S01, D2-S250-S02, D2-S250-S04, D2-S250-S08, D2-S250-S16, D2-S250-S32, D2-D250-B01, D2-D250-B02, D2-D250-B04, D2-D250-B08, D2-D250-B16, D2-D250-B32 and D2-D250-B64; Firmware Version: 4.0.0
1735	06/25/2012	IBM® z/VM® Version 6 Release 1 System SSL Cryptographic Module	IBM® Corporation	Hardware Version: z10 CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863; Software Version: 573FAL00: z/VM 6.1 with APAR PM43382
1736	06/21/2012	ProxySG 600-10 [1], 600-20 [2] and 600-35 [3]	Blue Coat Systems, Inc.	Hardware Versions: 090-02911 [1], 090-02912 [1], 090-02913 [2], 090-02914 [2], 090-02915 [3] and 090-02916 [3] with FIPS kit 085-02762; Firmware Version: 6.1

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
1737	06/25/2012	nShield F2 4000 [1], nShield F2 2000 [2] and nShield F2 500 [3]	Thales-eSecurity Inc.	Hardware Versions: nC3023P-4K0 [1], nC3023P-2K0 [2] and nC3123P-500 [3], Build Standard N; Firmware Version: 2.50.16-2
1738	06/25/2012	nToken	Thales-eSecurity Inc.	Hardware Version: nC2023P-000, Build Standard N; Firmware Version: 2.50.16-2
1739	06/25/2012	MiniHSM [1], MiniHSM for nShield Edge [2] and MiniHSM for Time Stamp Master Clock [3]	Thales-eSecurity Inc.	Hardware Versions: nC4031Z-10 [1], nC4031U-10 [2] and TSMC200 [3], Build Standard N; Firmware Version: 2.50.17-3
1740	06/25/2012	nShield F2 500 [1] and nShield F2 10 PCI [2]	Thales-eSecurity Inc.	Hardware Versions: nC3023P-500 [1] and nC3023P-10 [2], Build Standard N; Firmware Version: 2.50.16-2
1741	06/25/2012	nShield F3 500 [1], nShield F3 500 for NetHSM [2] and nShield F3 10 PCI [3]	Thales-eSecurity Inc.	Hardware Versions: nC4033P-500 [1], nC4033P-500N [2] and nC4033P-10 [3], Build Standard N; Firmware Version: 2.50.16-3
1742	06/25/2012	nShield F3 6000e [1], nShield F3 1500e [2], nShield F3 500e [3], nShield F3 10e [4], nShield F3 6000e for nShield Connect [5], nShield F3 1500e for nShield Connect [6] and nShield F3 500e for nShield Connect [7]	Thales-eSecurity Inc.	Hardware Versions: nC4033E-6K0 [1], nC4033E-1K5 [2], nC4033E-500 [3], nC4033E-030 [4], nC4033E-6K0N [5], nC4033E-1K5N [6] and nC4033E-500N [7], Build Standard N; Firmware Version: 2.50.16-3
1743	06/25/2012	nShield F2 6000e [1], nShield F2 1500e [2], nShield F2 500e [3] and nShield F2 10e [4]	Thales-eSecurity Inc.	Hardware Versions: nC3023E-6K0 [1], nC3023E-1K5 [2], nC3023E-500 [3] and nC3023E-010 [4], Build Standard N; Firmware Version: 2.50.16-2
1744	06/25/2012	MiniHSM [1], MiniHSM for nShield Edge [2] and MiniHSM for Time Stamp Master Clock [3]	Thales-eSecurity Inc.	Hardware Versions: nC4031Z-10 [1], nC3021U-10 [2] and TSMC200 [3], Build Standard N; Firmware Version: 2.50.17-2

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1745	06/25/2012	Vormetric Data Security Server Module	Vormetric Inc.	Hardware Version: 1.0; Firmware Version: 4.4.1
1746	06/25/2012	nShield F3 4000 [1], nShield F3 2000 [2], nShield F3 2000 for NetHSM [3], nShield F3 500 [4] and nShield F3 500 for NetHSM [5]	Thales-eSecurity Inc.	Hardware Versions: nC4033P-4K0 [1], nC4033P-2K0 [2], nC4033P-2K0N [3], nC4133P-500 [4] and nC4133P-500N [5], Build Standard N; Firmware Version: 2.50.16-2
1747	06/27/2012	OpenSSL FIPS Object Module	OpenSSL Software Foundation	Software Version: 2.0
1748	06/27/2012	BASICS IP PC104	Vocality International Ltd	Hardware Versions: 68551-01-1/68551C6; Firmware Version: 08_42.05
1751	06/27/2012	Astro Subscriber Motorola Advanced Crypto Engine (MACE)	Motorola Solutions, Inc.	Hardware Versions: P/Ns 5185912Y01 or 5185912Y03; Firmware Version: [D01.03.08 or R07.11.08] and [R01.00.00 or (R01.00.00 and R02.00.00)]
1752	06/27/2012	Astro Subscriber Motorola Advanced Crypto Engine (MACE)	Motorola Solutions, Inc.	Hardware Versions: P/Ns 5185912Y01 or 5185912Y03; Firmware Version: [D01.03.08 or R07.11.08] and [R01.00.00 or (R01.00.00 and R02.00.00)]