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