Do you have a link to the certificate for your FIPS ciphers?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, v7.2.8, v7.3.6 and later

QUESTION

Do you have a link to the certificate for your FIPS ciphers?

ANSWER

Globalscape EFT leverages the OpenSSL FIPS Object Module for all of its cryptographic functions while in FIPS mode. This module has been repeatedly certified by multiple organizations, and by extension, can be assumed to retain its FIPS-approved status no matter which organization or product adopts the OpenSSL FIPS module for its own use, when the module is used in its original (unaltered) form.

The FIPS module is distributed as a tar.gz source archive. The security policy document then contains sha-1 digest (which we check manually after downloading) and the exact steps to unpack and build the module. Our own build scripts follow the document to the letter, and this is why we can claim that we use a certified module. This is why we use gunzip.exe instead of the tools built into Windows and instead build the module using Visual Studio. This is what they said should be used.

The module itself contains tests that it runs each time it is loaded and initialized. The tests are sealed from outside code (including our EFT code and the non-certified parts of OpenSSL). During build the module is hashed in memory and the signature becomes hard coded into it. The signature is verified each time we load the module. The tests include some other tests of algorithms. The test inputs and outputs, however, are sealed. That is, we don’t modify the module, and it has internal tests to make sure it wasn’t modified afterwards.

More information about the OpenSSL FIPS Object Module can be found at these links:

- https://www.openssl.org/docs/fips.html
- Cryptographic Module Validation Program | CSRC (nist.gov)

Do you have a link to the certificate for your FIPS ciphers?

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11517/Do-you-have-a-link-to-the-ce...