Where cryptography is employed, what randomness source is used?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, all versions

QUESTION

Where cryptography is employed, what randomness source is used?

ANSWER

For SSL and related cryptography, we use the OpenSSL random number generator (technically, a pseudo-random number generator, or PRNG) which is based upon a seeded cryptographic hash function. This is documented here: https://www.openssl.org/docs/crypto/rand.html.

Our random number generation is FIPS compliant when operating in FIPS mode. The same random number generation technique is used in non-FIPS mode, it simply is the library implementation without the certification.

For SSH (SFTP) communications, the Crypto++ library is used, with its PNRG (which is also FIPS compliant and, when operated in the proper mode, FIPS certified).

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11190/Where-cryptography-is-employ...