From: Moody, Dustin (Fed)
To: Bassham, Lawrence E. (Fed)
Subject: aes ctr drbg in openssl
Date: Wednesday, August 2, 2017 2:26:58 PM

Larry,

Take a look at:

https://wiki.openssl.org/index.php/Random_Numbers

Scroll down to FIPS Mode, where it says:

FIPS mode is a special mode of operation which specifies the library should operate according to the security policies and procedures specified in FIPS 140-2. The mode requires use of the FIPS Capable OpenSSL library, and must be enabled with a call to `FIPS_mode_set`. Once in FIPS mode, a *default DRBG* is used as specified in SP800-90.

The default DRBG is 256-bit CTR AES using a derivation function, and is decided by the application and not the library module. In the case of an OpenSSL application it is specified in `rand_lib.c` via the `OPENSSL_DRBG_DEFAULT_TYPE` and `OPENSSL_DRBG_DEFAULT_FLAGS` preprocessor macros to allow them to be overridden by local compilation options or at runtime.

To use the FIPS random number generator, simply use `RAND_bytes` as described earlier. Note that the call to `FIPS_mode_set` must succeed in order to operate in FIPS 140 mode.

Dustin