Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'RAND_set_DRBG_type.3ossl' command

$ man RAND_set_DRBG_type.3ossl

RAND_SET_DRBG_TYPE(3ossl) OpenSSL RAND_SET_DRBG_TYPE(3ossl)

NAME

RAND_set_DRBG_type, RAND_set_seed_source_type - specify the global random number generator types

SYNOPSIS

```
#include <openssl/rand.h>

int RAND_set_DRBG_type(OSSL_LIB_CTX *ctx, const char *drbg, const char *propq,
                       const char *cipher, const char *digest);
int RAND_set_seed_source_type(OSSL_LIB_CTX *ctx, const char *seed,
                              const char *propq);
```

DESCRIPTION

RAND_set_DRBG_type() specifies the random bit generator that will be used within the library context ctx. A generator of name drbg with properties propq will be fetched. It will be instantiated with either cipher or digest as its underlying cryptographic algorithm. This specifies the type that will be used for the primary, public and private random instances.

RAND_set_seed_source_type() specifies the seed source that will be used

within the library context ctx. The seed source of name seed with properties propq will be fetched and used to seed the primary random big generator.

RETURN VALUES

These function return 1 on success and 0 on failure.

NOTES

These functions must be called before the random bit generators are first created in the library context. They will return an error if the call is made too late.

The default DRBG is "CTR-DRBG" using the "AES-256-CTR" cipher.

The default seed source is "SEED-SRC".

SEE ALSO

EVP_RAND(3), RAND_get0_primary(3)

HISTORY

These functions were added in OpenSSL 3.0.

COPYRIGHT

Copyright 2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.