



**Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!**

***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP RAND-TEST-RAND.7ssl'***

***\$ man EVP RAND-TEST-RAND.7ssl***

EVP RAND-TEST-RAND(7SSL)                      OpenSSL                      EVP RAND-TEST-RAND(7SSL)

**NAME**

EVP RAND-TEST-RAND - The test EVP RAND implementation

**DESCRIPTION**

Support for a test generator through the EVP RAND API. This generator is for test purposes only, it does not generate random numbers.

**Identity**

"TEST-RAND" is the name for this implementation; it can be used with the EVP RAND\_fetch() function.

**Supported parameters**

The supported parameters are:

"state" (OSSL RAND\_PARAM\_STATE) <integer>

These parameter works as described in "PARAMETERS" in EVP RAND(3).

"strength" (OSSL RAND\_PARAM\_STRENGTH) <unsigned integer>

"reseed\_requests" (OSSL DRBG\_PARAM\_RESEED\_REQUESTS) <unsigned integer>

"reseed\_time\_interval" (OSSL DRBG\_PARAM\_RESEED\_TIME\_INTERVAL) <integer>

"max\_request" (OSSL DRBG\_PARAM\_RESEED\_REQUESTS) <unsigned integer>

"min\_entropylen" (OSSL\_DRBG\_PARAM\_MIN\_ENTROPYLEN) <unsigned integer>  
"max\_entropylen" (OSSL\_DRBG\_PARAM\_MAX\_ENTROPYLEN) <unsigned integer>  
"min\_noncelen" (OSSL\_DRBG\_PARAM\_MIN\_NONCELEN) <unsigned integer>  
"max\_noncelen" (OSSL\_DRBG\_PARAM\_MAX\_NONCELEN) <unsigned integer>  
"max\_perslen" (OSSL\_DRBG\_PARAM\_MAX\_PERSLEN) <unsigned integer>  
"max\_adinlen" (OSSL\_DRBG\_PARAM\_MAX\_ADINLEN) <unsigned integer>  
"reseed\_counter" (OSSL\_DRBG\_PARAM\_RESEED\_COUNTER) <unsigned integer>

These parameters work as described in "PARAMETERS" in EVP RAND(3), except that they can all be set as well as read.

"test\_entropy" (OSSL\_RAND\_PARAM\_TEST\_ENTROPY) <octet string>

Sets the bytes returned when the test generator is sent an entropy request. The current position is remembered across generate calls. If there are insufficient data present to satisfy a call, an error is returned.

"test\_nonce" (OSSL\_RAND\_PARAM\_TEST\_NONCE) <octet string>

Sets the bytes returned when the test generator is sent a nonce request. Each nonce request will return all of the bytes.

## NOTES

A context for a test generator can be obtained by calling:

```
EVP_RAND *rand = EVP_RAND_fetch(NULL, "TEST-RAND", NULL);  
EVP_RAND_CTX *rctx = EVP_RAND_CTX_new(rand);
```

## EXAMPLES

```
EVP_RAND *rand;  
EVP_RAND_CTX *rctx;  
unsigned char bytes[100];  
OSSL_PARAM params[4], *p = params;  
unsigned char entropy[1000] = { ... };  
unsigned char nonce[20] = { ... };  
unsigned int strength = 48;
```

```
rand = EVP RAND_fetch(NULL, "TEST-RAND", NULL);
rctx = EVP RAND_CTX_new(rand, NULL);
EVP RAND_free(rand);

*p++ = OSSL_PARAM_construct_uint(OSSL RAND_PARAM_STRENGTH, &strength);
*p++ = OSSL_PARAM_construct_octet_string(OSSL RAND_PARAM_TEST_ENTROPY,
entropy, sizeof(entropy));
*p++ = OSSL_PARAM_construct_octet_string(OSSL RAND_PARAM_TEST_NONCE,
nonce, sizeof(nonce));
*p = OSSL_PARAM_construct_end();
EVP RAND_instantiate(rctx, strength, 0, NULL, 0, params);

EVP RAND_generate(rctx, bytes, sizeof(bytes), strength, 0, NULL, 0);

EVP RAND_CTX_free(rctx);
```

#### SEE ALSO

EVP RAND(3), "PARAMETERS" in EVP RAND(3)

#### COPYRIGHT

Copyright 2020-2021 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>>.