



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

### ***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP RAND-SEED-SRC.7ossl'***

***\$ man EVP RAND-SEED-SRC.7ossl***

EVP RAND-SEED-SRC(7ossl)      OpenSSL      EVP RAND-SEED-SRC(7ossl)

#### NAME

EVP RAND-SEED-SRC - The randomness seed source EVP RAND implementation

#### DESCRIPTION

Support for deterministic random number generator seeding through the EVP RAND API.

The seed sources used are specified at the time OpenSSL is configured for building using the --with-rand-seed= option. By default, operating system randomness sources are used.

#### Identity

"SEED-SRC" 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>

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

"max\_request" (OSSL\_RAND\_PARAM\_MAX\_REQUEST) <unsigned integer>

These parameters work as described in "PARAMETERS" in EVP\_RAND(3).

## NOTES

A context for the seed source can be obtained by calling:

```
EVP_RAND *rand = EVP_RAND_fetch(NULL, "SEED-SRC", NULL);
```

```
EVP_RAND_CTX *rctx = EVP_RAND_CTX_new(rand);
```

## EXAMPLES

```
EVP_RAND *rand;
```

```
EVP_RAND_CTX *seed, *rctx;
```

```
unsigned char bytes[100];
```

```
OSSL_PARAM params[2], *p = params;
```

```
unsigned int strength = 128;
```

```
/* Create a seed source */
```

```
rand = EVP_RAND_fetch(NULL, "SEED-SRC", NULL);
```

```
seed = EVP_RAND_CTX_new(rand, NULL);
```

```
EVP_RAND_free(rand);
```

```
/* Feed this into a DRBG */
```

```
rand = EVP_RAND_fetch(NULL, "CTR-DRBG", NULL);
```

```
rctx = EVP_RAND_CTX_new(rand, seed);
```

```
EVP_RAND_free(rand);
```

```
/* Configure the DRBG */
```

```
*p++ = OSSL_PARAM_construct_utf8_string(OSSL_DRBG_PARAM_CIPHER,  
SN_aes_256_ctr, 0);
```

```
*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);  
EVP RAND_CTX_free(seed);
```

#### 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>.

3.0.7                    2023-07-13        EVP RAND-SEED-SRC(7ossl)