



**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-HMAC-DRBG.7ssl'***

***\$ man EVP RAND-HMAC-DRBG.7ssl***

EVP RAND-HMAC-DRBG(7SSL)                      OpenSSL                      EVP RAND-HMAC-DRBG(7SSL)

**NAME**

EVP RAND-HMAC-DRBG - The HMAC DRBG EVP RAND implementation

**DESCRIPTION**

Support for the HMAC deterministic random bit generator through the EVP RAND API.

**Identity**

"HMAC-DRBG" 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>

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

"reseed\_time\_interval" (OSSL\_DRBG\_PARAM\_RESEED\_TIME\_INTERVAL) <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>  
"properties" (OSSL\_DRBG\_PARAM\_PROPERTIES) <UTF8 string>  
"mac" (OSSL\_DRBG\_PARAM\_MAC) <UTF8 string>  
"digest" (OSSL\_DRBG\_PARAM\_DIGEST) <UTF8 string>

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

## NOTES

A context for HMAC DRBG can be obtained by calling:

```
EVP_RAND *rand = EVP_RAND_fetch(NULL, "HMAC-DRBG", 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[3], *p = params;  
unsigned int strength = 128;  
  
rand = EVP_RAND_fetch(NULL, "HMAC-DRBG", NULL);  
rctx = EVP_RAND_CTX_new(rand, NULL);  
EVP_RAND_free(rand);  
  
*p++ = OSSL_PARAM_construct_utf8_string(OSSL_DRBG_PARAM_MAC, SN_hmac, 0);  
*p++ = OSSL_PARAM_construct_utf8_string(OSSL_DRBG_PARAM_DIGEST, SN_sha256, 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);
```

#### CONFORMING TO

NIST SP 800-90A and SP 800-90B

#### 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>.

3.0.2

2024-02-16

EVP RAND-HMAC-DRBG(7SSL)