

**NAME**

EVP RAND-HASH-DRBG – The HASH DRBG EVP RAND implementation

**DESCRIPTION**

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

**Identity**

“HASH-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>  
 “digest” (**OSSL DRBG\_PARAM\_DIGEST**) <UTF8 string>

These parameters work as described in “PARAMETERS” in **EVP RAND** (3).

**NOTES**

A context for HASH DRBG can be obtained by calling:

```
EVP RAND *rand = EVP RAND_fetch(NULL, "HASH-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[2], *p = params;
unsigned int strength = 128;

rand = EVP RAND_fetch(NULL, "HASH-DRBG", NULL);
rctx = EVP RAND_CTX_new(rand, NULL);
EVP RAND_free(rand);

*p++ = OSSL_PARAM_construct_utf8_string(OSSL_DRBG_PARAM_DIGEST, SN_sha512, 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>](https://www.openssl.org/source/license.html).