

NAME

EVP RAND-CTR-DRBG – The CTR DRBG EVP RAND implementation

DESCRIPTION

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

Identity

“CTR-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>
 “cipher” (**OSSL DRBG_PARAM_CIPHER**) <UTF8 string>

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

“use_derivation_function” (**OSSL DRBG_PARAM_USE_DF**) <integer>

This Boolean indicates if a derivation function should be used or not. A nonzero value (the default) uses the derivation function. A zero value does not.

NOTES

A context for CTR DRBG can be obtained by calling:

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

*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);
```

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).