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