



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

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'RAND_egd.3oss1' command

\$ man RAND_egd.3oss1

RAND_EGD(3oss1) OpenSSL RAND_EGD(3oss1)

NAME

RAND_egd, RAND_egd_bytes, RAND_query_egd_bytes - query entropy gathering daemon

SYNOPSIS

```
#include <openssl/rand.h>
```

```
int RAND_egd_bytes(const char *path, int num);
```

```
int RAND_egd(const char *path);
```

```
int RAND_query_egd_bytes(const char *path, unsigned char *buf, int num);
```

DESCRIPTION

On older platforms without a good source of randomness such as `/dev/urandom`, it is possible to query an Entropy Gathering Daemon (EGD) over a local socket to obtain randomness and seed the OpenSSL RNG. The protocol used is defined by the EGDs available at <http://egd.sourceforge.net/> or <http://prngd.sourceforge.net/>.

`RAND_egd_bytes()` requests `num` bytes of randomness from an EGD at the specified socket path, and passes the data it receives into `RAND_add()`.

RAND_egd() is equivalent to RAND_egd_bytes() with num set to 255.

RAND_query_egd_bytes() requests num bytes of randomness from an EGD at the specified socket path, where num must be less than 256. If buf is NULL, it is equivalent to RAND_egd_bytes(). If buf is not NULL, then the data is copied to the buffer and RAND_add() is not called.

OpenSSL can be configured at build time to try to use the EGD for seeding automatically.

RETURN VALUES

RAND_egd() and RAND_egd_bytes() return the number of bytes read from the daemon on success, or -1 if the connection failed or the daemon did not return enough data to fully seed the PRNG.

RAND_query_egd_bytes() returns the number of bytes read from the daemon on success, or -1 if the connection failed.

SEE ALSO

RAND_add(3), RAND_bytes(3), RAND(7)

COPYRIGHT

Copyright 2000-2018 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>.