NAME

RAND_set_rand_method, RAND_get_rand_method, RAND_OpenSSL – select RAND method

SYNOPSIS

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

RAND_METHOD *RAND_OpenSSL(void);

int RAND_set_rand_method(const RAND_METHOD *meth);

const RAND_METHOD *RAND_get_rand_method(void);
```

DESCRIPTION

A **RAND_METHOD** specifies the functions that OpenSSL uses for random number generation.

RAND_OpenSSL() returns the default **RAND_METHOD** implementation by OpenSSL. This implementation ensures that the PRNG state is unique for each thread.

If an **ENGINE** is loaded that provides the RAND API, however, it will be used instead of the method returned by **RAND_OpenSSL()**.

RAND_set_rand_method() makes **meth** the method for PRNG use. If an ENGINE was providing the method, it will be released first.

RAND_get_rand_method() returns a pointer to the current **RAND_METHOD**.

THE RAND_METHOD STRUCTURE

```
typedef struct rand_meth_st {
    int (*seed)(const void *buf, int num);
    int (*bytes)(unsigned char *buf, int num);
    void (*cleanup)(void);
    int (*add)(const void *buf, int num, double entropy);
    int (*pseudorand)(unsigned char *buf, int num);
    int (*status)(void);
} RAND_METHOD;
```

The fields point to functions that are used by, in order, **RAND_seed()**, **RAND_bytes()**, internal RAND cleanup, **RAND_add()**, **RAND_pseudo_rand()** and **RAND_status()**. Each pointer may be NULL if the function is not implemented.

RETURN VALUES

RAND_set_rand_method() returns 1 on success and 0 on failure. **RAND_get_rand_method()** and **RAND_OpenSSL()** return pointers to the respective methods.

SEE ALSO

RAND_bytes(3) , **ENGINE_by_id(3)** , **RAND(7)**

COPYRIGHT