NAME

RAND_load_file, RAND_write_file, RAND_file_name - PRNG seed file

SYNOPSIS

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

const char *RAND_file_name(char *buf, size_t num);

int RAND_load_file(const char *filename, long max_bytes);

int RAND_write_file(const char *filename);
```

DESCRIPTION

RAND_file_name() generates a default path for the random seed file. **buf** points to a buffer of size **num** in which to store the filename.

On all systems, if the environment variable **RANDFILE** is set, its value will be used as the seed file name.

Otherwise, the file is called ‘‘.rnd’’, found in platform dependent locations:

On Windows (in order of preference)
: `%HOME%`, `%USERPROFILE%`, `%SYSTEMROOT%`, C:\

On VMS
: SYS$LOGIN:

On all other systems
: `$HOME`

If `$HOME` (on non-Windows and non-VMS system) is not set either, or **num** is too small for the path name, an error occurs.

RAND_load_file() reads a number of bytes from file **filename** and adds them to the PRNG. If **max_bytes** is non-negative, up to **max_bytes** are read; if **max_bytes** is -1, the complete file is read.

RAND_write_file() writes a number of random bytes (currently 1024) to file **filename** which can be used to initialize the PRNG by calling *RAND_load_file()* in a later session.

RETURN VALUES

RAND_load_file() returns the number of bytes read or -1 on error.

RAND_write_file() returns the number of bytes written, and -1 if the bytes written were generated without appropriate seed.

RAND_file_name() returns a pointer to **buf** on success, and NULL on error.

SEE ALSO

rand(3) , *RAND_add(3)* , *RAND_cleanup(3)*

COPYRIGHT