NAME

openssl−rand, rand − generate pseudo−random bytes

SYNOPSIS

openssl rand [**−help**] [**−out** *file*] [**−rand file...**] [**−writerand file**] [**−base64**] [**−hex**] *num*

DESCRIPTION

This command generates *num* random bytes using a cryptographically secure pseudo random number generator (CSPRNG).

The random bytes are generated using the **RAND_bytes** (3) function, which provides a security level of 256 bits, provided it managed to seed itself successfully from a trusted operating system entropy source. Otherwise, the command will fail with a nonzero error code. For more details, see **RAND_bytes** (3), **RAND** (7), and **RAND_DRBG** (7).

OPTIONS

−help

Print out a usage message.

−out file

Write to *file* instead of standard output.

−rand file...

A file or files containing random data used to seed the random number generator. Multiple files can be specified separated by an OS-dependent character. The separator is **;** for MS-Windows, **,** for OpenVMS, and **:** for all others. Explicitly specifying a seed file is in general not necessary, see the ''NOTES'' section for more information.

[**−writerand file**]

Writes random data to the specified *file* upon exit. This can be used with a subsequent **−rand** flag.

−base64

Perform base64 encoding on the output.

−hex

Show the output as a hex string.

NOTES

Prior to OpenSSL 1.1.1, it was common for applications to store information about the state of the random-number generator in a file that was loaded at startup and rewritten upon exit. On modern operating systems, this is generally no longer necessary as OpenSSL will seed itself from a trusted entropy source provided by the operating system. The **−rand** and **−writerand** flags are still supported for special platforms or circumstances that might require them.

It is generally an error to use the same seed file more than once and every use of **−rand** should be paired with **−writerand**.

SEE ALSO

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

COPYRIGHT