NAME

gendsa - generate a DSA private key from a set of parameters

SYNOPSIS

openssl gendsa [**-out filename**] [**-aes128**] [**-aes192**] [**-aes256**] [**-camellia128**] [**-camellia192**] [**-camellia256**] [**-des**] [**-des3**] [**-idea**] [**-rand file(s)**] [**-engine id**] [**paramfile**]

DESCRIPTION

The **gendsa** command generates a DSA private key from a DSA parameter file (which will be typically generated by the **openssl dsaparam** command).

OPTIONS

-aes128|-aes192|-aes256|-camellia128|-camellia192|-camellia256|-des|-des3|-idea

These options encrypt the private key with specified cipher before outputting it. A pass phrase is prompted for. If none of these options is specified no encryption is used.

-rand file(s)

a file or files containing random data used to seed the random number generator, or an EGD socket (see *RAND_egd(3)*). Multiple files can be specified separated by a OS-dependent character. The separator is**;** for MS-Windo ws, **,** for OpenVMS, and **:** for all others.

-engine id

specifying an engine (by its unique **id** string) will cause **gendsa** to attempt to obtain a functional reference to the specified engine, thus initialising it if needed. The engine will then be set as the default for all available algorithms.

paramfile

This option specifies the DSA parameter file to use. The parameters in this file determine the size of the private key. DSA parameters can be generated and examined using the **openssl dsaparam** command.

NOTES

DSA key generation is little more than random number generation so it is much quicker that RSA key generation for example.

SEE ALSO

dsaparam(1), *dsa(1)*, *genrsa(1)*, *rsa(1)*