NAME

openssl−dsaparam, dsaparam − DSA parameter manipulation and generation

SYNOPSIS

openssl dsaparam [**−help**] [**−inform DER**|**PEM**] [**−outform DER**|**PEM**] [**−in filename**] [**−out filename**] [**−noout**] [**−text**] [**−C**] [**−rand file...**] [**−writerand file**] [**−genkey**] [**−engine id**] [**numbits**]

DESCRIPTION

This command is used to manipulate or generate DSA parameter files.

OPTIONS

−help

Print out a usage message.

−inform DER|**PEM**

This specifies the input format. The **DER** option uses an ASN1 DER encoded form compatible with RFC2459 (PKIX) DSS-Parms that is a SEQUENCE consisting of p, q and g respectively. The PEM form is the default format: it consists of the **DER** format base64 encoded with additional header and footer lines.

−outform DER|**PEM**

This specifies the output format, the options have the same meaning and default as the **−inform** option.

−in filename

This specifies the input filename to read parameters from or standard input if this option is not specified. If the **numbits** parameter is included then this option will be ignored.

−out filename

This specifies the output filename parameters to. Standard output is used if this option is not present. The output filename should **not** be the same as the input filename.

−noout

This option inhibits the output of the encoded version of the parameters.

−text

This option prints out the DSA parameters in human readable form.

−C This option converts the parameters into C code. The parameters can then be loaded by calling the **get_dsaXXX()** function.

−genkey

This option will generate a DSA either using the specified or generated parameters.

−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-W indows, **,** for OpenVMS, and **:** for all others.

[**−writerand file**]

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

numbits

This option specifies that a parameter set should be generated of size **numbits**. It must be the last option. If this option is included then the input file (if any) is ignored.

−engine id

Specifying an engine (by its unique **id** string) will cause **dsaparam** 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.

NOTES

PEM format DSA parameters use the header and footer lines:

```
-----BEGIN DSA PARAMETERS-----
-----END DSA PARAMETERS-----
```

DSA parameter generation is a slow process and as a result the same set of DSA parameters is often used to generate several distinct keys.

SEE ALSO

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

COPYRIGHT