NAME

dhparam - DH parameter manipulation and generation

SYNOPSIS

openssl dhparam [**-inform DER|PEM**] [**-outform DER|PEM**] [**-in** *filename*] [**-out** *filename*] [**-dsaparam**] [**-check**] [**-noout**] [**-text**] [**-C**] [**-2**] [**-5**] [**-rand** *file(s)*] [**-engine id**] [*numbits*]

DESCRIPTION

This command is used to manipulate DH parameter files.

OPTIONS

-inform DER|PEM

This specifies the input format. The **DER** option uses an ASN1 DER encoded form compatible with the PKCS#3 DHparameter structure. 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 as the **-inform** option.

-in *filename*

This specifies the input filename to read parameters from or standard input if this option is not specified.

-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.

-dsaparam

If this option is used, DSA rather than DH parameters are read or created; they are converted to DH format. Otherwise, "strong" primes (such that (p-1)/2 is also prime) will be used for DH parameter generation.

DH parameter generation with the **-dsaparam** option is much faster, and the recommended exponent length is shorter, which makes DH key exchange more efficient. Beware that with such DSA-style DH parameters, a fresh DH key should be created for each use to avoid small-subgroup attacks that may be possible otherwise.

-check

check if the parameters are valid primes and generator.

-2, **-5**

The generator to use, either 2 or 5. 2 is the default. If present then the input file is ignored and parameters are generated instead.

-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.

numbits

this option specifies that a parameter set should be generated of size *numbits*. It must be the last option. If not present then a value of 512 is used. If this option is present then the input file is ignored and parameters are generated instead.

-noout

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

-text

this option prints out the DH parameters in human readable form.

-C this option converts the parameters into C code. The parameters can then be loaded by calling the **get_dh***numbits***()** function.

-engine id
specifying an engine (by its unique **id** string) will cause **dhparam** 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.

WARNINGS

The program **dhparam** combines the functionality of the programs **dh** and **gendh** in previous versions of OpenSSL and SSLeay. The **dh** and **gendh** programs are retained for now but may have different purposes in future versions of OpenSSL.

NOTES

PEM format DH parameters use the header and footer lines:

```
-----BEGIN DH PARAMETERS-----
-----END DH PARAMETERS-----
```

OpenSSL currently only supports the older PKCS#3 DH, not the newer X9.42 DH.

This program manipulates DH parameters not keys.

BUGS

There should be a way to generate and manipulate DH keys.

SEE ALSO

dsaparam(1)

HISTORY

The **dhparam** command was added in OpenSSL 0.9.5. The **-dsaparam** option was added in OpenSSL 0.9.6.