



Rocky Enterprise Linux 9.2 Manual Pages on command 'dhparam.1ssl'

C:\>man dhparam.1ssl

DHPARAM(1SSL) OpenSSL DHPARAM(1SSL)

NAME

openssl-dhparam, dhparam - DH parameter manipulation and generation

SYNOPSIS

openssl dhparam [-help] [-inform DER|PEM] [-outform DER|PEM] [-in filename] [-out filename] [-dsaparam] [-check] [-noout] [-text] [-C] [-2] [-5] [-rand file...] [-writerand file] [-engine id] [numbits]

DESCRIPTION

This command is used to manipulate DH 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 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 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.

-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

Performs numerous checks to see if the supplied parameters are valid and displays a warning if not.

-2, -5

The generator to use, either 2 or 5. If present then the input file is ignored and parameters are generated instead. If not present but numbits is present, parameters are generated with the default generator 2.

-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.

[-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 present then the input file is ignored and parameters are generated instead. If this option is not present but

a generator (-2 or -5) is present, parameters are generated with a default length of 2048 bits.

-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_dhNNNN()` 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. 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)`

COPYRIGHT

Copyright 2000-2017 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the OpenSSL license (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file `LICENSE` in the source distribution or at <https://www.openssl.org/source/license.html>.