Rocky Enterprise Linux 9.2 Manual Pages on command 'openssl-dhparam.1ossl'

$ man openssl-dhparam.1ossl

OPENSSL-DHPARAM(1ossl) OpenSSL OPENSSL-DHPARAM(1ossl)

NAME

openssl-dhparam - DH parameter manipulation and generation

SYNOPSIS

openssl dhparam [-help] [-inform DER|PEM] [-outform DER|PEM] [-in filename] [-out filename] [-dsaparam] [-check] [-noout] [-text] [-2] [-3] [-5] [-engine id] [-rand files] [-writerand file] [-provider name] [-provider-path path] [-propquery propq] [numbits]

DESCRIPTION

This command is used to manipulate DH parameter files.

See "EXAMPLES" in openssl-genpkey(1) for examples on how to generate a key using a named safe prime group without generating intermediate parameters.

OPTIONS

-help

Print out a usage message.

-inform DER|PEM, -outform DER|PEM

The input format and output format; the default is PEM. The object

is compatible with the PKCS#3 DHparameter structure. See openssl-format-options(1) for details.

-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, -3, -5

The generator to use, either 2, 3 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.

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, -3 or -5) is present, parameters are generated with a default length of

2048 bits. The minimim length is 512 bits. The maximum length is 10000 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.

-engine id

See "Engine Options" in openssl(1). This option is deprecated.

-rand files, -writerand file

See "Random State Options" in openssl(1) for details.

-provider name

-provider-path path

-propquery propq

See "Provider Options" in openssl(1), provider(7), and property(7).

NOTES

This command replaces the dh and gendh commands of previous releases.

SEE ALSO

openssl(1), openssl-pkeyparam(1), openssl-dsaparam(1), openssl-genpkey(1).

HISTORY

The -engine option was deprecated in OpenSSL 3.0.

The -C option was removed in OpenSSL 3.0.

COPYRIGHT