

**NAME**

openssl-dsaparam - DSA parameter manipulation and generation

**SYNOPSIS**

**openssl dsaparam** [-help] [-inform DER|PEM] [-outform DER|PEM] [-in *filename*] [-out *filename*]  
[-noout] [-text] [-genkey] [-verbose] [-rand *files*] [-writerand *file*] [-engine *id*] [-provider *name*]  
[-provider-path *path*] [-propquery *propq*] [*numbits*]

**DESCRIPTION**

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

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

**OPTIONS****-help**

Print out a usage message.

**-inform DER|PEM**

The DSA parameters input format; unspecified by default. See **openssl-format-options(1)** for details.

**-outform DER|PEM**

The DSA parameters output format; the default is **PEM**. See **openssl-format-options(1)** for details.

Parameters are a sequence of **ASN.1 INTEGERS**: **p**, **q**, and **g**. This is compatible with RFC 2459 **DSS-Parms** structure.

**-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.

**-genkey**

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

**-verbose**

Print extra details about the operations being performed.

**-rand files, -writerand file**

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

**-engine id**

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

*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.

**-provider name****-provider-path path****-propquery propq**

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

**SEE ALSO**

**openssl(1)**, **openssl-pkeyparam(1)**, **openssl-gendsa(1)**, **openssl-dsa(1)**, **openssl-genrsa(1)**, **openssl-rsa(1)**

**HISTORY**

The **-engine** option was deprecated in OpenSSL 3.0.

The **-C** option was removed in OpenSSL 3.0.

**COPYRIGHT**

Copyright 2000-2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (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>.