NAME

openssl-dsa - DSA key processing

SYNOPSIS

openssl dsa [**-help**] [**-inform DER**|**PEM**] [**-outform DER**|**PEM**] [**-in** *filename*] [**-passin** *arg*] [**-out** *filename*] [**-passout** *arg*] [**-aes128**] [**-aes192**] [**-aes256**] [**-aria128**] [**-aria192**] [**-aria256**] [**-camellia128**] [**-camellia192**] [**-camellia256**] [**-des**] [**-des3**] [**-idea**] [**-text**] [**-noout**] [**-modulus**] [**-pubin**] [**-pubout**] [**-pvk-strong**] [**-pvk-weak**] [**-pvk-none**] [**-engine** *id*] [**-provider** *name*] [**-provider-path** *path*] [**-propquery** *propq*]

DESCRIPTION

This command processes DSA keys. They can be converted between various forms and their components printed out. **Note** This command uses the traditional SSLeay compatible format for private key encryption: newer applications should use the more secure PKCS#8 format using the **pkcs8**

OPTIONS

-help

Print out a usage message.

-inform DER|**PEM**

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

-outform DER|**PEM**

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

Private keys are a sequence of **ASN.1 INTEGERS**: the version (zero), **p**, **q**, **g**, and the public and private key components. Public keys are a **SubjectPublicKeyInfo** structure with the **DSA** type.

The **PEM** format also accepts PKCS#8 data.

-in *filename*

This specifies the input filename to read a key from or standard input if this option is not specified. If the key is encrypted a pass phrase will be prompted for.

-out *filename*

This specifies the output filename to write a key to or standard output by is not specified. If any encryption options are set then a pass phrase will be prompted for. The output filename should **not** be the same as the input filename.

-passin *arg*, **-passout** *arg*

The password source for the input and output file. For more information about the format of **arg** see **openssl-passphrase-options**(1).

-aes128, **-aes192**, **-aes256**, **-aria128**, **-aria192**, **-aria256**, **-camellia128**, **-camellia192**, **-camellia256**, **-des**, **-des3**, **-idea**

These options encrypt the private key with the specified cipher before outputting it. A pass phrase is prompted for. If none of these options is specified the key is written in plain text. This means that this command can be used to remove the pass phrase from a key by not giving any encryption option is given, or to add or change the pass phrase by setting them. These options can only be used with PEM format output files.

-text

Prints out the public, private key components and parameters.

-noout

This option prevents output of the encoded version of the key.

-modulus

This option prints out the value of the public key component of the key.

-pubin

By default, a private key is read from the input file. With this option a public key is read instead.

-pubout

By default, a private key is output. With this option a public key will be output instead. This option is automatically set if the input is a public key.

-pvk-strong

Enable 'Strong' PVK encoding level (default).

-pvk-weak

Enable 'Weak' PVK encoding level.

-pvk-none

Don't enforce PVK encoding.

-engine *id*

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

-provider *name*

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

The **openssl-pkey**(1) command is capable of performing all the operations this command can, as well as supporting other public key types.

EXAMPLES

The documentation for the **openssl-pkey**(1) command contains examples equivalent to the ones listed here.

To remove the pass phrase on a DSA private key:

```
openssl dsa -in key.pem -out keyout.pem
```

To encrypt a private key using triple DES:

```
openssl dsa -in key.pem -des3 -out keyout.pem
```

To convert a private key from PEM to DER format:

```
openssl dsa -in key.pem -outform DER -out keyout.der
```

To print out the components of a private key to standard output:

```
openssl dsa -in key.pem -text -noout
```

To just output the public part of a private key:

```
openssl dsa -in key.pem -pubout -out pubkey.pem
```

SEE ALSO

openssl(1), **openssl-pkey**(1), **openssl-dsaparam**(1), **openssl-gendsa**(1), **openssl-rsa**(1), **openssl-genrsa**(1)

HISTORY

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

COPYRIGHT