Rocky Enterprise Linux 9.2 Manual Pages on command 'openssl-pkey.1ssl'

C:\>man openssl-pkey.1ssl

PKEY(1SSL) OpenSSL PKEY(1SSL)

NAME

openssl-pkey, pkey - public or private key processing tool

SYNOPSIS

openssl pkey [-help] [-inform PEM|DER] [-outform PEM|DER] [-in filename] [-passin arg] [-out filename] [-passout arg] [-traditional] [-cipher] [-text] [-text_pub] [-noout] [-pubin] [-pubout] [-engine id] [-check] [-pubcheck]

DESCRIPTION

The pkey command processes public or private keys. They can be converted between various forms and their components printed out.

OPTIONS

-help

Print out a usage message.

-inform DER|PEM

This specifies the input format DER or PEM. The default format is PEM.

-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 a key from or standard input if this option is not specified. If the key is encrypted a pass phrase will be prompted for.

-passin arg

The input file password source. For more information about the format of arg see the PASS PHRASE ARGUMENTS section in openssl(1).

-out filename

This specifies the output filename to write a key to or standard output if this option 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.

-passout password

The output file password source. For more information about the format of arg see the PASS PHRASE ARGUMENTS section in openssl(1).

-traditional

Normally a private key is written using standard format: this is PKCS#8 form with the appropriate encryption algorithm (if any). If the -traditional option is specified then the older "traditional" format is used instead.

-cipher

These options encrypt the private key with the supplied cipher. Any algorithm name accepted by EVP_get_cipherbyname() is acceptable such as des3.

-text

Prints out the various public or private key components in plain text in addition to the encoded version.

-text_pub

Print out only public key components even if a private key is being processed.

-noout

Do not output the encoded version 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.

-engine id

Specifying an engine (by its unique id string) will cause pkey 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.

-check

This option checks the consistency of a key pair for both public and private components.

-pubcheck

This option checks the correctness of either a public key or the public component of a key pair.

EXAMPLES

To remove the pass phrase on an RSA private key:

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

To encrypt a private key using triple DES:

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

To convert a private key from PEM to DER format:

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

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

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

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

```
openssl pkey -in key.pem -text_pub -noout
```

To just output the public part of a private key:

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

SEE ALSO

genpkey(1), rsa(1), pkcs8(1), dsa(1), genrsa(1), gendsa(1)

COPYRIGHT