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

C:\>man openssl-rsa.1ssl

RSA(1SSL) OpenSSL RSA(1SSL)

NAME

openssl-rsa, rsa - RSA key processing tool

SYNOPSIS

openssl rsa [-help] [-inform PEM|DER] [-outform PEM|DER] [-in filename] [-passin arg] [-out filename] [-passout arg] [-aes128] [-aes192] [-aes256] [-aria128] [-aria192] [-aria256] [-camellia128] [-camellia192] [-camellia256] [-des] [-des3] [-idea] [-text] [-noout] [-modulus] [-check] [-pubin] [-pubout] [-RSAPublicKey_in] [-RSAPublicKey_out] [-engine id]

DESCRIPTION

The rsa command processes RSA 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 utility.

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#1 RSAPrivateKey or SubjectPublicKeyInfo format. The PEM form is the default format: it consists of the DER format base64 encoded with additional header and footer lines. On input PKCS#8 format private keys

are also accepted.

-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).

-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 using the rsa utility to read in an encrypted key with no encryption option can be used to remove the pass phrase from a key, or by setting the encryption options it can be use to add or change the pass phrase. These options can only be used with PEM format output files.

-text

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

-noout

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

-modulus

This option prints out the value of the modulus of the key.

-check

This option checks the consistency of an RSA private 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.

-RSAPublicKey_in, -RSAPublicKey_out

Like -pubin and -pubout except RSAPublicKey format is used instead.

-engine id

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

NOTES

The PEM private key format uses the header and footer lines:

-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----

The PEM public key format uses the header and footer lines:

-----BEGIN PUBLIC KEY-----

-----END PUBLIC KEY-----

The PEM RSAPublicKey format uses the header and footer lines:

-----BEGIN RSA PUBLIC KEY-----

-----END RSA PUBLIC KEY-----

EXAMPLES

To remove the pass phrase on an RSA private key:

openssl rsa -in key.pem -out keyout.pem

To encrypt a private key using triple DES:

openssl rsa -in key.pem -des3 -out keyout.pem

To convert a private key from PEM to DER format:

openssl rsa -in key.pem -outform DER -out keyout.der

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

openssl rsa -in key.pem -text -noout

To just output the public part of a private key:

openssl rsa -in key.pem -pubout -out pubkey.pem

Output the public part of a private key in RSAPublicKey format:

openssl rsa -in key.pem -RSAPublicKey_out -out pubkey.pem

BUGS

There should be an option that automatically handles .key files, without having to manually edit them.

SEE ALSO

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

COPYRIGHT