NAME

openssl-rsa - RSA key processing command

SYNOPSIS

openssl rsa [**-help**] [**-inform DER|PEM|P12|ENGINE**] [**-outform DER|PEM**] [**-in** *filename|uri*] [**-passin** *arg*] [**-out** *filename*] [**-passout** *arg*] [**-aes128**] [**-aes192**] [**-aes256**] [**-aria128**] [**-aria192**] [**-aria256**] [**-camellia128**] [**-camellia192**] [**-camellia256**] [**-des**] [**-des3**] [**-idea**] [**-text**] [**-noout**] [**-modulus**] [**-traditional**] [**-check**] [**-pubin**] [**-pubout**] [**-RSAPublicKey_in**] [**-RSAPublicKey_out**] [**-pvk-strong**] [**-pvk-weak**] [**-pvk-none**] [**-engine** *id*] [**-provider** *name*] [**-provider-path** *path*] [**-propquery** *propq*]

DESCRIPTION

This command processes RSA keys. They can be converted between various forms and their components printed out.

OPTIONS

-help

Print out a usage message.

-inform DER|PEM|P12|ENGINE

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.

-traditional

When writing a private key, use the traditional PKCS#1 format instead of the PKCS#8 format.

-in *filename|uri*

This specifies the input 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*, **-passout** *arg*

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

-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 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.

-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).

NOTES
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 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

openssl(1), **openssl-pkey**(1), **openssl-pkcs8**(1), **openssl-dsa**(1), **openssl-genrsa**(1), **openssl-gendsa**(1)

HISTORY

The **-engine** option was deprecated 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>.