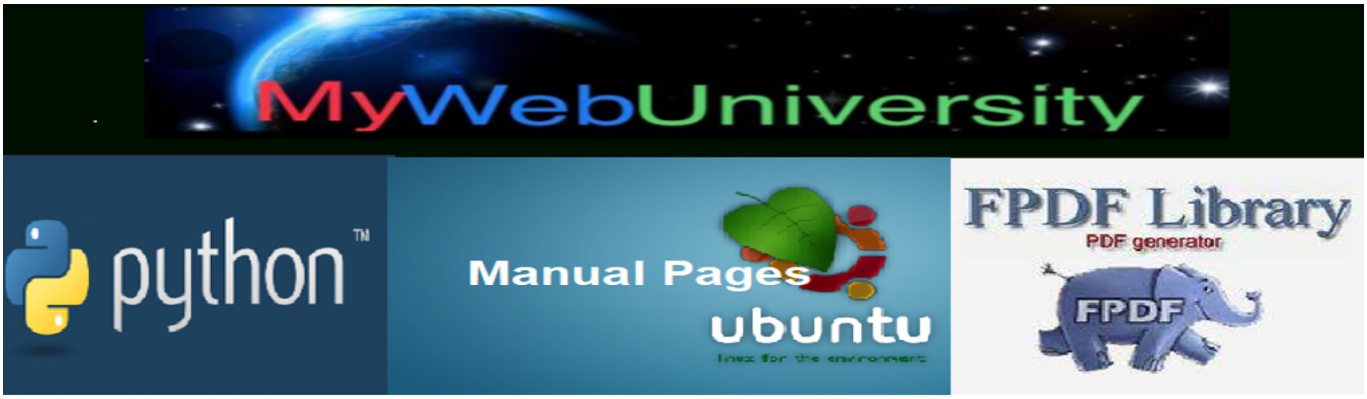

Rocky Enterprise Linux 9.2 Manual Pages on command 'openssl-pkey.1ssl'

$ man openssl-pkey.1ssl

OPENSSL-PKEY(1SSL) OpenSSL OPENSSL-PKEY(1SSL)

NAME

openssl-pkey - public or private key processing command

SYNOPSIS

openssl pkey [-help] [-engine id] [-provider name] [-provider-path path] [-propquery propq] [-check] [-pubcheck] [-in filename|uri] [-inform DER|PEM|P12|ENGINE] [-passin arg] [-pubin] [-out filename] [-outform DER|PEM] [-cipher] [-passout arg] [-traditional] [-pubout] [-noout] [-text] [-text_pub] [-ec_conv_form arg] [-ec_param_enc arg]

DESCRIPTION

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

OPTIONS

General options

-help

Print out a usage message.

-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).

-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.

Input options

-in filename|uri

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

-inform DER|PEM|P12|ENGINE

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

-passin arg

The password source for the key input.

For more information about the format of arg see openssl-passphrase-options(1).

-pubin

By default a private key is read from the input. With this option only the public components are read.

Output options

-out filename

This specifies the output filename to save the encoded and/or text output of key or standard output if this option is not specified. If any cipher option is set but no -passout is given then a pass phrase will be prompted for. The output filename should not be the same as the input filename.

-outform DER|PEM

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

-cipher

Encrypt the PEM encoded private key with the supplied cipher. Any algorithm name accepted by EVP_get_cipherbyname() is acceptable such as aes128. Encryption is not supported for DER output.

-passout arg

The password source for the output file.

For more information about the format of arg see openssl-passphrase-options(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.

-pubout

By default the private and public key is output; this option restricts the output to the public components. This option is automatically set if the input is a public key. When combined with -text, this is equivalent to -text_pub.

-noout

Do not output the key in encoded form.

-text

Output the various key components in plain text (possibly in addition to the PEM encoded form). This cannot be combined with encoded output in DER format.

-text_pub

Output in text form only the public key components (also for private keys). This cannot be combined with encoded output in DER format.

-ec_conv_form arg

This option only applies to elliptic-curve based keys.

This specifies how the points on the elliptic curve are converted into octet strings. Possible values are: compressed (the default value), uncompressed and hybrid. For more information regarding the point conversion forms please read the X9.62 standard. Note Due to patent issues the compressed option is disabled by default for binary curves and can be enabled by defining the preprocessor macro OPENSSL_EC_BIN_PT_COMP at compile time.

-ec_param_enc arg

This option only applies to elliptic curve based public and private keys.

This specifies how the elliptic curve parameters are encoded. Possible value are: named_curve, i.e. the ec parameters are specified by an OID, or explicit where the ec parameters are explicitly given (see RFC 3279 for the definition of the EC parameters structures). The default value is named_curve. Note the implicitlyCA alternative, as specified in RFC 3279, is currently not implemented in OpenSSL.

EXAMPLES

To remove the pass phrase on a 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

To change the EC parameters encoding to explicit:

openssl pkey -in key.pem -ec_param_enc explicit -out keyout.pem

To change the EC point conversion form to compressed:

openssl pkey -in key.pem -ec_conv_form compressed -out keyout.pem

SEE ALSO

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

HISTORY

The -engine option was deprecated in OpenSSL 3.0.

COPYRIGHT