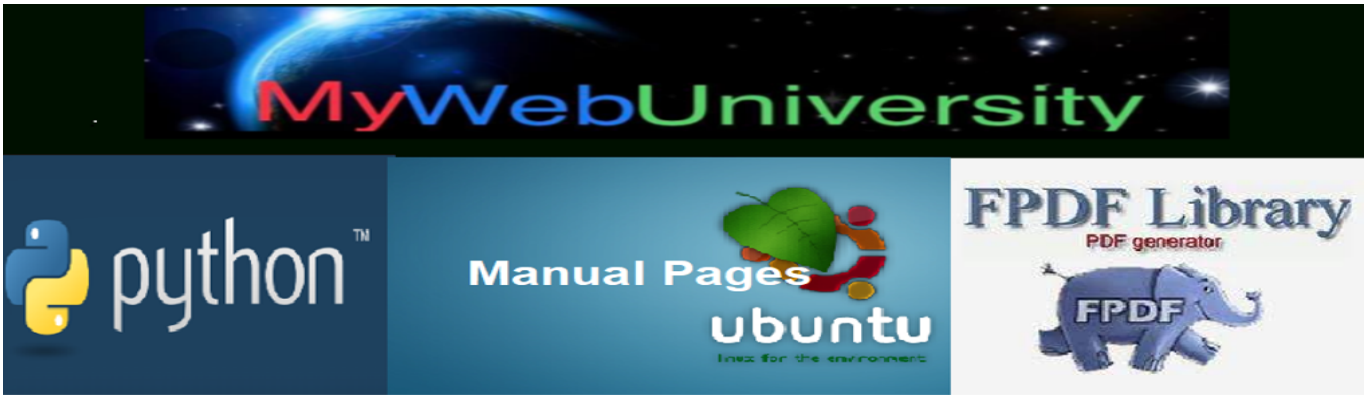

Rocky Enterprise Linux 9.2 Manual Pages on command 'openssl-spkac.1ssl'

$ man openssl-spkac.1ssl

OPENSSL-SPKAC(1SSL) OpenSSL OPENSSL-SPKAC(1SSL)

NAME

openssl-spkac - SPKAC printing and generating command

SYNOPSIS

openssl spkac [-help] [-in filename] [-out filename] [-digest digest] [-key filename|uri] [-keyform DER|PEM|P12|ENGINE] [-passin arg] [-challenge string] [-pubkey] [-spkac spkacname] [-spksect section] [-noout] [-verify] [-engine id] [-provider name] [-provider-path path] [-propquery propq]

DESCRIPTION

This command processes Netscape signed public key and challenge (SPKAC) files. It can print out their contents, verify the signature and produce its own SPKACs from a supplied private key.

OPTIONS

-help

Print out a usage message.

-in filename

This specifies the input filename to read from or standard input if this option is not specified. Ignored if the -key option is used.

-out filename

Specifies the output filename to write to or standard output by default.

-digest digest

Use the specified digest to sign a created SPKAC file. The default digest algorithm is MD5.

-key filename|uri

Create an SPKAC file using the private key specified by filename or uri. The -in, -noout, -spksect and -verify options are ignored if present.

-keyform DER|PEM|P12|ENGINE

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

-passin arg

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

-challenge string

Specifies the challenge string if an SPKAC is being created.

-spkac spkacname

Allows an alternative name form the variable containing the SPKAC. The default is "SPKAC". This option affects both generated and input SPKAC files.

-spksect section

Allows an alternative name form the section containing the SPKAC. The default is the default section.

-noout

Don't output the text version of the SPKAC (not used if an SPKAC is being created).

-pubkey

Output the public key of an SPKAC (not used if an SPKAC is being created).

-verify

Verifies the digital signature on the supplied SPKAC.

-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).

EXAMPLES

Print out the contents of an SPKAC:

```
openssl spkac -in spkac.cnf
```

Verify the signature of an SPKAC:

```
openssl spkac -in spkac.cnf -noout -verify
```

Create an SPKAC using the challenge string "hello":

```
openssl spkac -key key.pem -challenge hello -out spkac.cnf
```

Example of an SPKAC, (long lines split up for clarity):

```
SPKAC=MIG5MGUwXDANBgkqhkiG9w0BAQEFAANLADBIAkEA\
1cCoq2Wa3Ixs47uI7FPVwHVIPDx5yso105Y6zpozam135a\
8R0CpoRvkkigIyXfcCjiVi5oWk+6FfPaD03uPFoQIDAQAB\
FgVoZWxsbzANBgkqhkiG9w0BAQQFAANBAFpQtY/FojdwkJ\
h1bEIYuc2EeM2KHTWPEepWYeawvHD0gQ3DngSC75YCWnnD\
dq+NQ3F+X4deMx9AaEglZtULwV4=
```

NOTES

A created SPKAC with suitable DN components appended can be fed to openssl-ca(1).

SPKACs are typically generated by Netscape when a form is submitted containing the KEYGEN tag as part of the certificate enrollment process.

The challenge string permits a primitive form of proof of possession of private key. By checking the SPKAC signature and a random challenge string some guarantee is given that the user knows the private key corresponding to the public key being certified. This is important in some applications. Without this it is possible for a previous SPKAC to be used in a "replay attack".

SEE ALSO

openssl(1), openssl-ca(1)

HISTORY

The -engine option was deprecated in OpenSSL 3.0.

The -digest option was added in OpenSSL 3.0.

COPYRIGHT