NAME

openssl-crl2pkcs7 - Create a PKCS#7 structure from a CRL and certificates

SYNOPSIS

openssl crl2pkcs7 [**-help**] [**-inform DER|PEM**] [**-outform DER|PEM**] [**-in** *filename*] [**-out** *filename*]
[**-certfile** *filename*] [**-nocrl**] [**-provider** *name*] [**-provider-path** *path*] [**-propquery** *propq*]

DESCRIPTION

This command takes an optional CRL and one or more certificates and converts them into a PKCS#7
degenerate "certificates only" structure.

OPTIONS

-help

Print out a usage message.

-inform DER|PEM

The input format of the CRL; the default is **PEM**. See **openssl-format-options**(1) for details.

-outform DER|PEM

The output format of the PKCS#7 object; the default is **PEM**. See **openssl-format-options**(1) for
details.

-in *filename*

This specifies the input filename to read a CRL from or standard input if this option is not
specified.

-out *filename*

Specifies the output filename to write the PKCS#7 structure to or standard output by default.

-certfile *filename*

Specifies a filename containing one or more certificates in **PEM** format. All certificates in the file
will be added to the PKCS#7 structure. This option can be used more than once to read certificates
from multiple files.

-nocrl

Normally a CRL is included in the output file. With this option no CRL is included in the output
file and a CRL is not read from the input file.

-provider *name*
-provider-path *path*

-propquery *propq*

    See "Provider Options" in **openssl**(1), **provider**(7), and **property**(7).

EXAMPLES

Create a PKCS#7 structure from a certificate and CRL:

 openssl crl2pkcs7 -in crl.pem -certfile cert.pem -out p7.pem

Creates a PKCS#7 structure in DER format with no CRL from several different certificates:

 openssl crl2pkcs7 -nocrl -certfile newcert.pem
    -certfile demoCA/cacert.pem -outform DER -out p7.der

NOTES

The output file is a PKCS#7 signed data structure containing no signers and just certificates and an optional CRL.

This command can be used to send certificates and CAs to Netscape as part of the certificate enrollment process. This involves sending the DER encoded output as MIME type application/x-x509-user-cert.

The **PEM** encoded form with the header and footer lines removed can be used to install user certificates and CAs in MSIE using the Xenroll control.

SEE ALSO

openssl(1), **openssl-pkcs7**(1)

COPYRIGHT