

**NAME**

cr1 - CRL utility

**SYNOPSIS**

```
openssl cr1 [-inform PEM|DER] [-outform PEM|DER] [-text] [-in filename] [-out filename] [-nameopt option] [-noout] [-hash] [-issuer] [-lastupdate] [-nextupdate] [-CAfile file] [-CApath dir]
```

**DESCRIPTION**

The **cr1** command processes CRL files in DER or PEM format.

**COMMAND OPTIONS****-inform DER|PEM**

This specifies the input format. **DER** format is DER encoded CRL structure. **PEM** (the default) is a base64 encoded version of the DER form with header and footer lines.

**-outform DER|PEM**

This specifies the output format, the options have the same meaning as the **-inform** option.

**-in filename**

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

**-out filename**

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

**-text**

print out the CRL in text form.

**-nameopt option**

option which determines how the subject or issuer names are displayed. See the description of **-nameopt** in *x509(1)*.

**-noout**

don't output the encoded version of the CRL.

**-hash**

output a hash of the issuer name. This can be use to lookup CRLs in a directory by issuer name.

**-hash\_old**

outputs the "hash" of the CRL issuer name using the older algorithm as used by OpenSSL versions before 1.0.0.

**-issuer**

output the issuer name.

**-lastupdate**

output the lastUpdate field.

**-nextupdate**

output the nextUpdate field.

**-CAfile file**

verify the signature on a CRL by looking up the issuing certificate in **file**

**-CApath dir**

verify the signature on a CRL by looking up the issuing certificate in **dir**. This directory must be a standard certificate directory: that is a hash of each subject name (using **x509 -hash**) should be linked to each certificate.

**NOTES**

The PEM CRL format uses the header and footer lines:

```
-----BEGIN X509 CRL-----
-----END X509 CRL-----
```

**EXAMPLES**

Convert a CRL file from PEM to DER:

```
openssl crl -in crl.pem -outform DER -out crl.der
```

Output the text form of a DER encoded certificate:

```
openssl crl -in crl.der -text -noout
```

**BUGS**

Ideally it should be possible to create a CRL using appropriate options and files too.

**SEE ALSO**

[crl2pkcs7\(1\)](#), [ca\(1\)](#), [x509\(1\)](#)