

NAME

`c_rehash` - Create symbolic links to files named by the hash values

SYNOPSIS

```
c_rehash [-old] [-h] [-n] [-v] [ directory...]
```

DESCRIPTION

`c_rehash` scans directories and calculates a hash value of each `.pem`, `.crt`, `.cer`, or `.crl` file in the specified directory list and creates symbolic links for each file, where the name of the link is the hash value. (If the platform does not support symbolic links, a copy is made.) This utility is useful as many programs that use OpenSSL require directories to be set up like this in order to find certificates.

If any directories are named on the command line, then those are processed in turn. If not, then the `SSL_CERT_DIR` environment variable is consulted; this should be a colon-separated list of directories, like the Unix `PATH` variable. If that is not set then the default directory (installation-specific but often `/usr/local/ssl/certs`) is processed.

In order for a directory to be processed, the user must have write permissions on that directory, otherwise it will be skipped. The links created are of the form `HHHHHHHH.D`, where each `H` is a hexadecimal character and `D` is a single decimal digit. When processing a directory, `c_rehash` will first remove all links that have a name in that syntax. If you have links in that format used for other purposes, they will be removed. To skip the removal step, use the `-n` flag. Hashes for CRL's look similar except the letter `r` appears after the period, like this: `HHHHHHHH.rD`.

Multiple objects may have the same hash; they will be indicated by incrementing the `D` value. Duplicates are found by comparing the full SHA-1 fingerprint. A warning will be displayed if a duplicate is found.

A warning will also be displayed if there are files that cannot be parsed as either a certificate or a CRL.

The program uses the `openssl` program to compute the hashes and fingerprints. If not found in the user's `PATH`, then set the `OPENSSL` environment variable to the full pathname. Any program can be used, it will be invoked as follows for either a certificate or CRL:

```
$OPENSSL x509 -hash -fingerprint -noout -in FILENAME  
$OPENSSL crl -hash -fingerprint -noout -in FILENAME
```

where `FILENAME` is the filename. It must output the hash of the file on the first line, and the fingerprint on the second, optionally prefixed with some text and an equals sign.

OPTIONS

`-old`

Use old-style hashing (MD5, as opposed to SHA-1) for generating links for releases before 1.0.0. Note that current versions will not use the old style.

`-h` Display a brief usage message.

`-n` Do not remove existing links. This is needed when keeping new and old-style links in the same directory.

`-v` Print messages about old links removed and new links created. By default, `c_rehash` only lists each directory as it is processed.

ENVIRONMENT

`OPENSSL`

The path to an executable to use to generate hashes and fingerprints (see above).

`SSL_CERT_DIR`

Colon separated list of directories to operate on. Ignored if directories are listed on the command line.

SEE ALSO

openssl(1), *crl(1)*, *x509(1)*.