Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'dirmngr-client.1'

$ man dirmngr-client.1

DIRMNGR-CLIENT(1)   GNU Privacy Guard 2.2   DIRMNGR-CLIENT(1)

NAME

    dirmngr-client - Tool to access the Dirmngr services

SYNOPSIS

    dirmngr-client [options] [certfile|pattern]

DESCRIPTION

    The dirmngr-client is a simple tool to contact a running dirmngr and

    test whether a certificate has been revoked --- either by being listed

    in the corresponding CRL or by running the OCSP protocol. If no dirm?

    ngr is running, a new instances will be started but this is in general

    not a good idea due to the huge performance overhead.

    The usual way to run this tool is either:

      dirmngr-client acert

    or

      dirmngr-client <acert

    Where acert is one DER encoded (binary) X.509 certificates to be

    tested.

RETURN VALUE

dirmngr-client returns these values:

0   The certificate under question is valid; i.e. there is a valid

CRL available and it is not listed there or the OCSP request re?

turned that that certificate is valid.

1   The certificate has been revoked

2 (and other values)

There was a problem checking the revocation state of the cer?

tificate.   A message to stderr has given more detailed informa?

tion. Most likely this is due to a missing or expired CRL or

due to a network problem.

OPTIONS

dirmngr-client may be called with the following options:

--version

Print the program version and licensing information. Note that

you cannot abbreviate this command.

--help, -h

Print a usage message summarizing the most useful command-line

options. Note that you cannot abbreviate this command.

--quiet, -q

Make the output extra brief by suppressing any informational

messages.

-v

--verbose

Outputs additional information while running. You can increase

the verbosity by giving several verbose commands to dirmngr,

such as ?-vv?.

--pem Assume that the given certificate is in PEM (armored) format.

--ocsp Do the check using the OCSP protocol and ignore any CRLs.

--force-default-responder

When checking using the OCSP protocol, force the use of the de?

fault OCSP responder. That is not to use the Reponder as given

by the certificate.

--ping Check whether the dirmngr daemon is up and running.

--cache-cert

   Put the given certificate into the cache of a running dirmngr.

   This is mainly useful for debugging.

--validate

   Validate the given certificate using dirmngr's internal valida?

   tion code. This is mainly useful for debugging.

--load-crl

   This command expects a list of filenames with DER encoded CRL

   files.   With the option --url URLs are expected in place of

   filenames and they are loaded directly from the given location.

   All CRLs will be validated and then loaded into dirmngr's cache.

--lookup

   Take the remaining arguments and run a lookup command on each of

   them. The results are Base-64 encoded outputs (without header

   lines). This may be used to retrieve certificates from a

   server. However the output format is not very well suited if

   more than one certificate is returned.

--url

-u   Modify the lookup and load-crl commands to take an URL.

--local

-l   Let the lookup command only search the local cache.

--squid-mode

   Run dirmngr-client in a mode suitable as a helper program for

   Squid's external_acl_type option.

SEE ALSO

dirmngr(8), gpgsm(1)

The full documentation for this tool is maintained as a Texinfo manual.

If GnuPG and the info program are properly installed at your site, the

command

   info gnupg

should give you access to the complete manual including a menu struc?

ture and an index.