NAME

pki --verify - Verify a certificate using a CA certificate

SYNOPSIS

pki --verify[**--in** *file*] [**--cacert** *file*] [**--crl** *file*] [**--debug** *level*] [**--online**]

pki --verify--options *file*

pki --verify-h | **--help**

DESCRIPTION

This sub-command of **pki**(1) verifies a certificate using an optional CA certificate.

OPTIONS

-h, --help

Print usage information with a summary of the available options.

-v, --debug *level*

Set debug level, default: 1.

-+, --options *file*

Read command line options from *file*.

-i, --in *file*

X.509 certificate to verify. If not given it is read from *STDIN*.

-c, --cacert *file*

CA certificate to use for trustchain verification. If not given the certificate is assumed to be self-signed. May optionally be a path to a directory from which CA certificates are loaded. Can be used multiple times.

-l, --crl *file*

Local CRL to use for trustchain verification. May optionally be a path to a directory from which CRLs are loaded. Can be used multiple times. Implies **-o**.

-o, --online

Enable online CRL/OCSP revocation checking.

EXIT STATUS

The exit status is 0 if the certificate was verified successfully, 1 if the certificate is untrusted, 2 if the

certificate’s lifetimes are invalid, and 3 if the certificate was verified successfully but the online revocation check indicated that it has been revoked.

SEE ALSO

pki(1)