NAME

openssl-verify - certificate verification command

SYNOPSIS

openssl verify [**-help**] [**-CRLfile** *filename|uri*] [**-crl_download**] [**-show_chain**] [**-verbose**] [**-trusted** *filename|uri*] [**-untrusted** *filename|uri*] [**-vfyopt** *nm:v*] [**-nameopt** *option*] [**-CAfile** *file*] [**-no-CAfile**] [**-CApath** *dir*] [**-no-CApath**] [**-CAstore** *uri*] [**-no-CAstore**] [**-engine** *id*] [**-allow_proxy_certs**] [**-attime** *timestamp*] [**-no_check_time**] [**-check_ss_sig**] [**-crl_check**] [**-crl_check_all**] [**-explicit_policy**] [**-extended_crl**] [**-ignore_critical**] [**-inhibit_any**] [**-inhibit_map**] [**-partial_chain**] [**-policy** *arg*] [**-policy_check**] [**-policy_print**] [**-purpose** *purpose*] [**-suiteB_128**] [**-suiteB_128_only**] [**-suiteB_192**] [**-trusted_first**] [**-no_alt_chains**] [**-use_deltas**] [**-auth_level** *num*] [**-verify_depth** *num*] [**-verify_email** *email*] [**-verify_hostname** *hostname*] [**-verify_ip** *ip*] [**-verify_name** *name*] [**-x509_strict**] [**-issuer_checks**] [**-provider** *name*] [**-provider-path** *path*] [**-propquery** *propq*] [**--**] [*certificate ...*]

DESCRIPTION

This command verifies certificate chains. If a certificate chain has multiple problems, this program attempts to display all of them.

OPTIONS

-help

Print out a usage message.

-CRLfile *filename|uri*

The file or URI should contain one or more CRLs in PEM or DER format. This option can be specified more than once to include CRLs from multiple sources.

-crl_download

Attempt to download CRL information for certificates via their CDP entries.

-show_chain

Display information about the certificate chain that has been built (if successful). Certificates in the chain that came from the untrusted list will be flagged as "untrusted".

-verbose

Print extra information about the operations being performed.

-trusted *filename|uri*

A file or URI of (more or less) trusted certificates. See **openssl-verification-options**(1) for more information on trust settings.

This option can be specified more than once to load certificates from multiple sources.

-untrusted *filename|uri*

A file or URI of untrusted certificates to use for chain building. This option can be specified more than once to load certificates from multiple sources.

-vfyopt *nm*:*v*

Pass options to the signature algorithm during verify operations. Names and values of these options are algorithm-specific.

-nameopt *option*

This specifies how the subject or issuer names are displayed. See **openssl-namedisplay-options**(1) for details.

-engine *id*

See "Engine Options" in **openssl**(1). This option is deprecated.

To load certificates or CRLs that require engine support, specify the **-engine** option before any of the **-trusted**, **-untrusted** or **-CRLfile** options.

-CAfile *file*, **-no-CAfile**, **-CApath** *dir*, **-no-CApath**, **-CAstore** *uri*, **-no-CAstore**

See "Trusted Certificate Options" in **openssl-verification-options**(1) for details.

-allow_proxy_certs, **-attime**, **-no_check_time**, **-check_ss_sig**, **-crl_check**, **-crl_check_all**, **-explicit_policy**, **-extended_crl**, **-ignore_critical**, **-inhibit_any**, **-inhibit_map**, **-no_alt_chains**, **-partial_chain**, **-policy**, **-policy_check**, **-policy_print**, **-purpose**, **-suiteB_128**, **-suiteB_128_only**, **-suiteB_192**, **-trusted_first**, **-use_deltas**, **-auth_level**, **-verify_depth**, **-verify_email**, **-verify_hostname**, **-verify_ip**, **-verify_name**, **-x509_strict** **-issuer_checks**

Set various options of certificate chain verification. See "Verification Options" in **openssl-verification-options**(1) for details.

-provider *name*
-provider-path *path*
-propquery *propq*

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

-- Indicates the last option. All arguments following this are assumed to be certificate files. This is useful if the first certificate filename begins with a **-**.

certificate ...

One or more target certificates to verify, one per file. If no certificates are given, this command will attempt to read a single certificate from standard input.

DIAGNOSTICS

When a verify operation fails the output messages can be somewhat cryptic. The general form of the error message is:

```
server.pem: /C=AU/ST=Queensland/O=CryptSoft Pty Ltd/CN=Test CA (1024 bit)
error 24 at 1 depth lookup:invalid CA certificate
```

The first line contains the name of the certificate being verified followed by the subject name of the certificate. The second line contains the error number and the depth. The depth is number of the certificate being verified when a problem was detected starting with zero for the target ("leaf") certificate itself then 1 for the CA that signed the target certificate and so on. Finally a textual version of the error number is presented.

A list of the error codes and messages can be found in **X509_STORE_CTX_get_error**(3); the full list is defined in the header file <*openssl/x509_vfy.h*>.

This command ignores many errors, in order to allow all the problems with a certificate chain to be determined.

SEE ALSO

openssl-verification-options(1), **openssl-x509**(1), **ossl_store-file**(7)

HISTORY

The **-show_chain** option was added in OpenSSL 1.1.0.

The **-engine option** was deprecated in OpenSSL 3.0.

COPYRIGHT