NAME

trust – Tool for operating on the trust policy store

SYNOPSIS

trust list

trust extract ––filter=<what> ––format=<type> /path/to/destination

trust anchor /path/to/certificate.crt

trust dump

DESCRIPTION

trust is a command line tool to examine and modify the shared trust policy store.

See the various sub commands below. The following global options can be used:

–v, ––verbose
Run in verbose mode with debug output.

–q, ––quiet
Run in quiet mode without warning or failure messages.

LIST

List trust policy store items.

```
$ trust list
```

List information about the various items in the trust policy store. Each item is listed with it's PKCS#11 URI and some descriptive information.

You can specify the following options to control what to list.

––filter=<what>
Specifies what certificates to extract. You can specify the following values:

ca–anchors
Certificate anchors

trust–policy
Anchors and blacklist (default)

blacklist
Blacklisted certificates

certificates
All certificates

pkcs11:object=xx
A PKCS#11 URI to filter with

If an output format is chosen that cannot support type what has been specified by the filter, a message will be printed.

None of the available formats support storage of blacklist entries that do not contain a full certificate. Thus any certificates blacklisted by their issuer and serial number alone, are not included in the extracted blacklist.

––purpose=<usage>
Limit to certificates usable for the given purpose You can specify one of the following values:

server–auth
For authenticating servers

client–auth
For authenticating clients

email
For email protection

code−signing
For authenticated signed code

1.2.3.4.5...
An arbitrary purpose OID

ANCHOR

Store or remove trust anchors.

```
$ trust anchor /path/to/certificate.crt
$ trust anchor −−remove /path/to/certificate.crt
$ trust anchor −−remove "pkcs11:id=%AA%BB%CC%DD%EE;type=cert"
```

Store or remove trust anchors in the trust policy store. These are usually root certificate authorities.

Specify either the **−−store** or **−−remove** operations. If no operation is specified then **−−store** is assumed.

When storing, one or more certificate files are expected on the command line. These are stored as anchors, unless they are already present.

When removing an anchor, either specify certificate files or PKCS#11 URI's on the command line. Matching anchors will be removed.

It may be that this command needs to be run as root in order to modify the system trust policy store, if no user specific store is available.

You can specify the following options.

−−remove
Remove one or more anchors from the trust policy store. Specify certificate files or PKCS#11 URI's on the command line.

−−store
Store one or more anchors to the trust policy store. Specify certificate files on the command line.

EXTRACT

Extract trust policy from the shared trust policy store.

```
$ trust extract −−format=x509−directory −−filter=ca−anchors /path/to/directory
```

You can specify the following options to control what to extract. The **−−filter** and **−−format** arguments should be specified. By default this command will not overwrite the destination file or directory.

−−comment
Add identifying comments to PEM bundle output files before each certificate.

−−filter=<what>
Specifies what certificates to extract. You can specify the following values:

ca−anchors
Certificate anchors (default)

trust−policy
Anchors and blacklist

blacklist
Blacklisted certificates

certificates
All certificates

pkcs11:object=xx

A PKCS#11 URI

If an output format is chosen that cannot support type what has been specified by the filter, a message will be printed.

None of the available formats support storage of blacklist entries that do not contain a full certificate. Thus any certificates blacklisted by their issuer and serial number alone, are not included in the extracted blacklist.

−−format=<type>
The format of the destination file or directory. You can specify one of the following values:

x509−file
DER X.509 certificate file

x509−directory
directory of X.509 certificates

pem−bundle
File containing one or more certificate PEM blocks

pem−directory
Directory of PEM files each containing one certificate

pem−directory−hash
Directory of PEM files each containing one certificate, with hash symlinks

openssl−bundle
OpenSSL specific PEM bundle of certificates

openssl−directory
Directory of OpenSSL specific PEM files

java−cacerts
Java keystore 'cacerts' certificate bundle

−−overwrite
Overwrite output file or directory.

−−purpose=<usage>
Limit to certificates usable for the given purpose You can specify one of the following values:

server−auth
For authenticating servers

client−auth
For authenticating clients

email
For email protection

code−signing
For authenticated signed code

1.2.3.4.5...
An arbitrary purpose OID

EXTRACT COMPAT

Extract compatibility trust certificate bundles.

```
$ trust extract−compat
```

OpenSSL, Java and some versions of GnuTLS cannot currently read trust information directly from the trust policy store. This command extracts trust information such as certificate anchors for use by these libraries.

What this command does, and where it extracts the files is distribution or site specific. Packagers or administrators are expected customize this command.

DUMP

Dump PKCS#11 items in the various tokens.

```
$ trust dump
```

Dump information about the various PKCS#11 items in the tokens. Each item is dumped with it's PKCS#11 URI and information in the .p11−kit persistence format.

You can specify the following options to control what to dump.

−−filter=<what>

Specifies what certificates to extract. You can specify the following values:

all

All objects. This is the default

pkcs11:object=xx

A PKCS#11 URI to filter with

BUGS

Please send bug reports to either the distribution bug tracker or the upstream bug tracker at **https://github.com/p11−glue/p11−kit/issues/**.

SEE ALSO

p11-kit(8)

An explanatory document about storing trust policy: **https://p11−glue.github.io/p11−glue/doc/storing−trust−policy/**

Further details available in the p11−kit online documentation at **https://p11−glue.github.io/p11−glue/p11−kit/manual/**.