

NAME

p11-kit - Tool for operating on configured PKCS#11 modules

SYNOPSIS

p11-kit list-modules

p11-kit list-tokens ...

p11-kit list-objects ...

p11-kit import-object ...

p11-kit export-object ...

p11-kit delete-object ...

p11-kit generate-keypair ...

p11-kit list-profiles ...

p11-kit add-profile ...

p11-kit delete-profile ...

p11-kit list-mechanisms ...

p11-kit print-config

p11-kit extract ...

p11-kit server ...

DESCRIPTION

p11-kit is a command line tool that can be used to perform operations on PKCS#11 modules configured on the system.

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 MODULES

List system configured PKCS#11 modules.

```
$ p11-kit list-modules
```

The modules, information about them and the tokens present in the PKCS#11 modules will be displayed.

LIST TOKENS

List all tokens available in system configured PKCS#11 modules.

```
$ p11-kit list-tokens [--only-uris] pkcs11:token
```

This retrieves all tokens and displays some of their common attributes. If **--only-uris** is given, only the matching token URIs are printed.

LIST OBJECTS

List objects matching given PKCS#11 URI.

```
$ p11-kit list-objects [--login] pkcs11:object_on_token
```

This retrieves all objects that match given PKCS#11 URI and displays some of their common attributes. Storage objects also have their PKCS#11 URI displayed.

IMPORT OBJECT

Import object into PKCS#11 token.

```
$ p11-kit import-object --file=file.pem [--label=label] [--login] pkcs11:token
```

Takes either an X.509 certificate or a public key in the form of a PEM file and imports it into the first token matched by given PKCS#11 URI.

--file=<file.pem>

File containing either an X.509 certificate or a public key in PEM format. This option is required.

--label=<label>

Assigns label to the imported object.

EXPORT OBJECT

Export object matching PKCS#11 URI.

```
$ p11-kit export-object [--login] pkcs11:object_on_token
```

Displays PEM formatted contents of the first object matched by given PKCS#11 URI. The matched object has to either be an X.509 certificate or a public key.

DELETE OBJECT

Delete object matching PKCS#11 URI.

```
$ p11-kit delete-object [--login] pkcs11:object_on_token
```

Destroys the first object matched by given PKCS#11 URI.

GENERATE KEY-PAIR

Generate key-pair on a PKCS#11 token.

```
$ p11-kit generate-keypair --type=algorithm {--bits=n|--curve=name} [--label=label] [--login] pkcs11:token
```

Generate private-public key-pair of given type on the first token matched by given PKCS#11 URI. This command should be used together with --type option and one of --bits or --curve options.

--type=<algorithm>

Specify the type of keys to generate. Supported values are rsa, ecdsa and ed25519. This option is required.

--bits=<n>

Specify the number of bits for the key-pair generation. Cannot be used together with --curve option.

--curve=<name>

Specify an elliptic curve for the key-pair generation. Supported values are secp256r1, secp384r1, secp521r1, ed25519 and ed448. Cannot be used together with --bits option.

--label=<label>

Assigns label to the generated key-pair objects.

LIST PROFILES

List PKCS#11 profiles supported by the token.

```
$ p11-kit list-profiles [--login] pkcs11:token
```

Displays profile IDs of the first token matched by given PKCS#11 URI in human-readable form.

ADD PROFILE

Add PKCS#11 profile to a token.

```
$ p11-kit add-profile --profile=profile [--login] pkcs11:token
```

Creates new profile object with given profile ID on the first token matched by given PKCS#11 URI. This command fails if the profile ID already exists on the token.

--profile=<profile>

Profile ID to add. Value can either be numerical or textual. This option is required.

DELETE PROFILE

Delete PKCS#11 profile from a token.

```
$ p11-kit delete-profile --profile=profile [--login] pkcs11:token
```

Destroys all profile objects with given profile ID from the first token matched by given PKCS#11 URI.

--profile=<profile>

Profile ID to delete. Value can either be numerical or textual. This option is required.

LIST MECHANISMS

List PKCS#11 mechanisms supported by the token.

```
$ p11-kit list-mechanisms pkcs11:token
```

This lists all available mechanisms for a PKCS#11 token

PRINT CONFIG

Print merged configuration.

```
$ p11-kit print-config
```

P11-kit provides 3 levels of configuration: system wide, per-module, and per-user. At run-time all 3 levels are merged into a single configuration. This command displays the merged configuration.

EXTRACT

Extract certificates from configured PKCS#11 modules.

This operation has been moved to a separate command **trust extract**. See **trust(1)** for more information

SERVER

Run a server process that exposes PKCS#11 module remotely.

```
$ p11-kit server pkcs11:token1 pkcs11:token2 ...
```

```
$ p11-kit server --provider /path/to/pkcs11-module.so pkcs11:token1 pkcs11:token2 ...
```

This launches a server that exposes the given PKCS#11 tokens on a local socket. The tokens must belong to the same module. To access the socket, use `p11-kit-client.so` module. The server address and PID are printed as a shell-script snippet which sets the appropriate environment variable: `P11_KIT_SERVER_ADDRESS` and `P11_KIT_SERVER_PID`.

EXTRACT TRUST

Extract standard trust information files.

This operation has been moved to a separate command **trust extract-compat**. See **trust(1)** for more information

REMOTE

Run a PKCS#11 module remotely.

```
$ p11-kit remote /path/to/pkcs11-module.so
```

```
$ p11-kit remote pkcs11:token1 pkcs11:token2 ...
```

This is not meant to be run directly from a terminal. But rather in a **remote** option in a **pkcs11.conf(5)** file.

This exposes the given PKCS#11 module or tokens over standard input and output. Those two forms, whether to expose a module or tokens, are mutually exclusive and if the second form is used, the tokens must belong to the same module.

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

pkcs11.conf(5)

Further details available in the p11-kit online documentation at <https://p11-glue.github.io/p11-glue/p11-kit/manual/>.