

**NAME**

`pki --pkcs7` - Provides PKCS#7 wrap/unwrap functions

**SYNOPSIS**

`pki --pkcs7--sign|--verify|--encrypt|--decrypt|--show` [`--in file`] [`--cert file`] [`--key file`] [`--digest digest`]  
[`--rsa-padding padding`] [`--debug level`]

`pki --pkcs7--options file`

`pki --pkcs7-h | --help`

**DESCRIPTION**

This sub-command of `pki(1)` provides functions to wrap/unwrap PKCS#7 containers.

**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*.

**-s, --sign**

Create PKCS#7 signed-data.

**-u, --verify**

Verify PKCS#7 signed-data.

**-e, --encrypt**

Create PKCS#7 enveloped-data.

**-e, --decrypt**

Decrypt PKCS#7 enveloped-data.

**-p, --show**

Show information about PKCS#7 container, list certificates.

**-i, --in file**

PKCS#7 input file. If not given the input is read from *STDIN*.

**-k, --key file**

Private key used for **--sign** and **--decrypt**.

**-c, --cert file**

Certificate for **--sign**, **--verify** and **--encrypt**. Can be used multiple times.

**-g, --digest digest**

Digest to use for signature creation. One of *md5*, *sha1*, *sha224*, *sha256*, *sha384*, or *sha512*. The default is determined based on the type and size of the signature key.

**-R, --rsa-padding padding**

Padding to use for RSA signatures. Either *pkcs1* or *pss*, defaults to *pkcs1*.

**SEE ALSO**

**pki(1)**