

**NAME**

`pki --keyid` - Calculate key identifiers of a key or certificate

**SYNOPSIS**

`pki --keyid`[`--in file`|`--keyid hex`] [`--type type`] [`--id id-type`] [`--format format`] [`--debug level`]

`pki --keyid--options file`

`pki --keyid-h | --help`

**DESCRIPTION**

This sub-command of `pki(1)` calculates key identifiers of private keys and certificates.

**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**

Input file. If not given the input is read from *STDIN*.

**-x, --keyid hex**

Smartcard or TPM private key object handle in hex format with an optional 0x prefix.

**-t, --type type**

Type of input. One of *priv* (private key), *rsa* (RSA private key), *ecdsa* (ECDSA private key), *bliss* (BLISS private key), *pub* (public key), *pkcs10* (PKCS#10 certificate request), *x509* (X.509 certificate), defaults to *priv*.

**-I, --id id-type**

Type of identifier. One of *all* (all identifiers), *spk* (SHA-1 hash of subjectPublicKey), *spki* (SHA-1 hash of subjectPublicKeyInfo), defaults to *all*.

**-f, --format format**

Output format. One of *pretty* (user-readable output), *hex* (hexadecimal encoding), *base64* (Base64

encoding), *bin* (raw binary data), defaults to *pretty*.

## EXAMPLES

Calculate key identifiers of an RSA private key:

```
$ pki --keyid --in key.der
subjkey (SHA-1 of subjectPublicKey):
    6a:9c:74:d1:f8:89:79:89:f6:5a:94:e9:89:f1...
keyid (SHA-1 of subjectPublicKeyInfo):
    6e:55:dc:7e:9c:a5:58:d9:5b:e3:c7:13:14:e1...
```

Calculate key identifiers of an X.509 certificate:

```
$ pki --keyid --in cert.der --type x509
subjkey (SHA-1 of subjectPublicKey):
    6a:9c:74:d1:f8:89:79:89:f6:5a:94:e9:89:f1...
keyid (SHA-1 of subjectPublicKeyInfo):
    6e:55:dc:7e:9c:a5:58:d9:5b:e3:c7:13:14:e1...
```

Calculate keyid in simple hex encoding of an X.509 certificate:

```
$ pki --keyid --in cert.der --type x509 --id spki --format hex
6e55dc7e9ca558d95be3c71314e1...
```

## SEE ALSO

**pki(1)**