

**NAME**

**pki --signcrl** - Issue a Certificate Revocation List (CRL) using a CA certificate and key

**SYNOPSIS**

```
pki --signcrl--cakey file|--cakeyid hex --cacert file [--lifetime days] [--this-update datetime]  
    [--next-update datetime] [--lastcrl crl] [--basecrl crl] [--crluri uri] [--digest digest]  
    [--rsa-padding padding] [--reason reason] [--date ts] --cert file|--serial hex] [--critical oid]  
    [--outform encoding] [--debug level]
```

**pki --signcrl--options** *file*

**pki --signcrl-h | --help**

**DESCRIPTION**

This sub-command of **pki(1)** is used to issue a Certificate Revocation List (CRL) using a CA certificate and private key.

**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*.

**-k, --cakey** *file*

CA private key file. Either this or **--cakeyid** is required.

**-x, --cakeyid** *hex*

Smartcard or TPM CA private key object handle in hex format with an optional 0x prefix. Either this or **--cakey** is required.

**-c, --cacert** *file*

CA certificate file. Required.

**-l, --lifetime** *days*

Days until the CRL gets a nextUpdate, default: 15. Ignored if both an absolute start and end time are given.

**-F, --this-update** *datetime*

Absolute time when the validity of the CRL begins. The datetime format is defined by the **--dateform** option.

**-T, --next-update** *datetime*

Absolute time when the validity of the CRL end. The datetime format is defined by the **--dateform** option.

**-D, --dateform** *form*

strptime(3) format for the **--this-update** and **--next-update** options, default: **%d.%m.%y %T**

**-a, --lastcrl** *crl*

CRL of lastUpdate to copy revocations from.

**-b, --basecrl** *crl*

Base CRL to create a delta CRL for.

**-u, --crluri** *uri*

Freshest delta CRL URI to include in CRL. 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*.

**-X, --critical** *oid*

Add a critical extension with the given OID.

**-f, --outform** *encoding*

Encoding of the created certificate file. Either *der* (ASN.1 DER) or *pem* (Base64 PEM), defaults to *der*.

**Revoked Certificates**

Multiple revoked certificates can be added to the CRL by either providing the certificate file or the respective serial number directly. A reason and a timestamp can be configured for each revocation (they have to be given before each certificate/serial on the command line).

**-r, --reason** *reason*

The reason why the certificate was revoked. One of *key-compromise*, *ca-compromise*, *affiliation-changed*, *superseded*, *cessation-of-operation*, or *certificate-hold*.

**-d, --date** *ts*

Revocation date as Unix timestamp. Defaults to the current time.

**-z, --cert** *file*

Certificate file to revoke.

**-s, --serial** *hex*

Hexadecimal encoded serial number of the certificate to revoke.

## EXAMPLES

Revoke a certificate:

```
pki --signcrl --cacert ca_cert.der --cakey ca_key.der \  
--reason superseded --cert cert.der > crl.der
```

Update an existing CRL with two new revocations, using the certificate's serial number, but no reason:

```
pki --signcrl --cacert ca_cert.der --cakey ca_key.der \  
--lastcrl old_crl.der --serial 0123 --serial 0345 > crl.der
```

## SEE ALSO

**pki(1)**