NAME

pki --scep - Enroll an X.509 certificate with a SCEP server

SYNOPSIS

pki --scep--url *url* [**--in** *file*] [**--dn** *distinguished-name*] [**--san** *subjectAltName*] [**--profile** *profile*]
[**--password** *password*] **--ca-cert-enc** *file* **--ca-cert-sig** *file* [**--cacert** *file*] **[--cert** *file* **--key** *file***]**
[**--cipher** *cipher*] [**--digest** *digest*] [**--rsa-padding** *padding*] [**--interval** *time*]
[**--maxpolltime** *time*] [**--outform** *encoding*] [**--debug** *level*]

pki --scep--options *file*

pki --scep-h | **--help**

DESCRIPTION

This sub-command of **pki**(1) sends a PKCS#10 certificate request in an encrypted and signed PKCS#7 container via HTTP to a SCEP server using the Simple Certificate Enrollment Protocol (RFC 8894). After successful authorization which with manual authentication requires periodic polling by the enrollment client, the SCEP server returns an X.509 certificate signed by the CA.

Before the expiry of the current certificate, a new client certificate based on a fresh RSA private key can be requested, using the old certificate and the old key for automatic authentication with the SCEP server.

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*.

-u, --url *url*
URL of the SCEP server.

-i, --in *file*
RSA private key. If not given the key is read from *STDIN*.

-d, --dn *distinguished-name*

Subject distinguished name (DN). Required unless --cert is given.

-a, --san *subjectAltName*
subjectAltName extension to include in request. Can be used multiple times.

-P, --profile *profile*
Certificate profile name to be included in the certificate request. Can be any UTF8 string. Supported e.g. by the **openxpki** SCEP server with profiles (*pc-client*, *tls-server*, etc.) that are translated into corresponding Extended Key Usage (EKU) flags in the generated X.509 certificate.

-p, --password *password*
The challengePassword to include in the certificate request.

-e, --cacert-enc *file*
CA or RA certificate for encryption

-s, --cacert-sig *file*
CA certificate for signature verification

-C, --cacert *file*
Additional CA certificate in the trust chain used for signature verification. Can be used multiple times.

-c, --cert *file*
Client certificate to be renewed.

-k, --key *file*
Client RSA private key to be replaced.

-E, --cipher *cipher*
Cipher used for symmetric encryption. Either *aes* (the default) or *des3*.

-g, --digest *digest*
Digest to use for signature creation. One of *sha256* (the default), *sha384*, *sha512*, or *sha1*.

-R, --rsa-padding *padding*
Padding to use for RSA signatures. Either *pkcs1* (the default) or *pss*.

-t, --interval *time*
Poll interval in seconds, defaults to *60s*.

-m, --maxpolltime *time*
Maximum poll time in seconds, defaults to *0* which means unlimited polling.

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

EXAMPLES

To save some typing work the following command line options are stored in a *scep.opt* file:

```
--url http://pki.strongswan.org:8080/scep
--cacert-enc myra.crt
--cacert-sig myca-1.crt
--cacert myca.crt
```

With the following command, an X.509 certificate signed by the intermediate CA is requested from a SCEP server:

```
pki --options scep.opt --in moonKey.der --san "moon.strongswan.org" \
   --dn "C=CH, O=strongSec GmbH, CN=moon.strongswan.org" > moonCert.der

transaction ID: 4DFCF31CB18A9B5333CCEC6F99CF230E4524E334
  using certificate "C=CH, O=strongSwan Project, CN=SCEP RA"
  using trusted intermediate ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Issuing CA"
  using trusted ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Root CA"
  reached self-signed root ca with a path length of 1
  SCEP request pending, polling indefinitely every 60 seconds
  going to sleep for 60 seconds
transaction ID: 4DFCF31CB18A9B5333CCEC6F99CF230E4524E334
  ...
  going to sleep for 60 seconds
Issued certificate "C=CH, O=strongSwan Project, CN=moon.strongswan.org"
  serial: 1e:ff:22:7b:6e:d7:4c:c1:8a:06
  using certificate "C=CH, O=strongSwan Project, CN=moon.strongswan.org"
  using trusted intermediate ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Issuing CA"
  using trusted ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Root CA"
  reached self-signed root ca with a path length of 1
Issued certificate is trusted, valid from Aug 22 18:56:23 2022 until Aug 22 18:56:23 2023 (currently valid)
```

A certificate about to expire can be renewed with the command:

```
pki --options scep.opt --in moonNewKey.der --san "moon.strongswan.org" \
   --dn "C=CH, O=strongSec GmbH, CN=moon.strongswan.org" \
   --cert moonCert.der --key moonKey.der > moonNewCert.der

transaction ID: A9A63D028CC439F68452D125C4DBA025E67DBA95
  using certificate "C=CH, O=strongSwan Project, CN=SCEP RA"
  using trusted intermediate ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Issuing CA"
  using trusted ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Root CA"
  reached self-signed root ca with a path length of 1
Issued certificate "C=CH, O=strongSwan Project, CN=moon.strongswan.org"
  serial: 1f:ff:b2:78:43:a2:9d:85:00:38
  using certificate "C=CH, O=strongSwan Project, CN=moon.strongswan.org"
  using trusted intermediate ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Issuing CA"
  using trusted ca certificate "C=CH, O=strongSwan Project, CN=strongSwan Root CA"
  reached self-signed root ca with a path length of 1
Issued certificate is trusted, valid from Jul 20 15:05:33 2023 until Jul 20 15:05:33 2024 (currently valid)
```

SEE ALSO

pki(1)