NAME

pki --acert - Issue an attribute certificate

SYNOPSIS

pki --acert[**--in** *file*] [**--group** *membership*] **--issuerkey** *file*|**--issuerkeyid** *hex* **--issuercert** *file*
[**--lifetime** *hours*] [**--not-before** *datetime*] [**--not-after** *datetime*] [**--serial** *hex*] [**--digest** *digest*]
[**--rsa-padding** *padding*] [**--outform** *encoding*] [**--debug** *level*]

pki --acert--options *file*

pki --acert-h | **--help**

DESCRIPTION

This sub-command of **pki**(1) is used to issue an attribute certificate using an issuer certificate with its private key and the holder certificate.

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*
Holder certificate to issue an attribute certificate for. If not given the certificate is read from *STDIN*.

-m, --group *membership*
Group membership the attribute certificate shall certify. The specified group is included as a string. To include multiple groups, the option can be repeated.

-k, --issuerkey *file*
Issuer private key file. Either this or **--issuerkeyid** is required.

-x, --issuerkeyid *hex*
Smartcard or TPM issuer private key object handle in hex format with an optional h0x prefix. Either this or **--issuerkey** is required.

-c, --issuercert *file*
Issuer certificate file. Required.

-l, --lifetime *hours*
Hours the attribute certificate is valid, default: 24. Ignored if both an absolute start and end time are given.

-F, --not-before *datetime*
Absolute time when the validity of the AC begins. The datetime format is defined by the **--dateform** option.

-T, --not-after *datetime*
Absolute time when the validity of the AC ends. The datetime format is defined by the **--dateform** option.

-D, --dateform *form*
strptime(3) format for the **--not-before** and **--not-after** options, default: **%d.%m.%y %T**

-s, --serial *hex*
Serial number in hex. It is randomly allocated by default.

-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*.

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

EXAMPLES

To save repetitive typing, command line options can be stored in files. Lets assume *acert.opt* contains the following contents:

```
--issuercert aacert.der --issuerkey aakey.der --digest sha256 --lifetime 4
```

Then the following command can be used to issue an attribute certificate based on a holder certificate and the options above:

```
pki --acert --options acert.opt --in holder.der --group sales --group finance -f pem
```

SEE ALSO

pki(1)