Certificates

Overview

Certificate manager is used to:

- collecting all certificates inside the router;
- manage and create self-signed certificates;
- control and set SCEP related configuration.;

Starting from RouterOS version 6 certificate validity is shown using local time zone offset. In previous versions it was UTF.

General Menu

```
/certificate
```

General menu is used to manage certificates, add templates, issue certificates and manage SCEP Clients.

Certificate Template

Certificate templates are deleted right after certificate issue or certificate request command is executed:

```
/certificate
add name=CA-Template common-name=CAtemp key-usage=key-cert-sign,crl-sign
add name=Server common-name=server
add name=Client common-name=client
```

Let`s print out certificates:

```
[admin@4k11] /certificate> print detail
Flags: K - private-key; L - crl; C - smart-card-key; A - authority; I - issued, R - revoked; E - expired; T -
trusted
 0         name="CA-Template" key-type=rsa common-name="CAtemp" key-size=2048 subject-alt-name="" days-
valid=365 key-usage=key-cert-sign,crl-sign

 1         name="Server" key-type=rsa common-name="server" key-size=2048 subject-alt-name="" days-valid=365
           key-usage=digital-signature,key-encipherment,data-encipherment,key-cert-sign,crl-sign,tls-server,tls-
client

 2         name="Client" key-type=rsa common-name="client" key-size=2048 subject-alt-name="" days-valid=365
           key-usage=digital-signature,key-encipherment,data-encipherment,key-cert-sign,crl-sign,tls-server,tls-
client
```

⚠ If CA certificate is removed then all issued certificates in the chain are also removed.

Sign Certificate

Certificates should be signed. In the following example, we will sign certificates and add CRL URL for the server certificate:

```
/certificate
sign CA-Template
sign Client
sign Server ca-crl-host=192.168.88.1 name=ServerCA
```

Let`s check is certificates are signed:

```
[admin@MikroTik] /certificate> print
Flags: K - private-key; L - crl; A - authority; T - trusted
Columns: NAME, COMMON-name, FINGERPRINT
#        NAME         COMMON  FINGERPRINT
0  K AT  CA-Template  CAtemp  0c7aaa7607a4dde1bbf33deaae6be7bac9fe4064ba47d64e8a73dcefad6cfc38
1  K AT  Client       client  b3ff25ecb166ea41e15733a7493003f3ea66310c10390c33e98fe32364c3659f
2  KLAT  ServerCA     server  152b88c9d81f4b765a59e2302e01efd1fbf11ceeed6e59f4974e87787a5bb980
```


The time of the key signing process depends on key-size of a specific certificate. With values 4k and higher, it might take a substantial time to sign this specific certificate on less powerful CPU based devices.

Export Certificate

It is possible to export client certificates with keys and CA certificate:

```
/certificate
export-certificate CA-Template
export-certificate ServerCA export-passphrase=yourpassphrase
export-certificate Client export-passphrase=yourpassphrase
```

Exported certificates are available under */file* section:

```
[admin@MikroTik] > file print
Columns: NAME, TYPE, SIZE, CREATION-TIME
#  NAME                        TYPE        SIZE  CREATION-TIME
0  skins                       directory         jan/19/2019 00:00:04
1  flash                       directory         jan/19/2019 01:00:00
2  flash/rw                    directory         jan/19/2019 01:00:00
3  flash/rw/disk               directory         jan/19/2019 01:00:00
4  pub                         directory         jan/19/2019 02:42:16
5  cert_export_CA-Template.crt  .crt file   1119  jan/19/2019 04:15:21
6  cert_export_ServerCA.crt     .crt file   1229  jan/19/2019 04:15:42
7  cert_export_ServerCA.key     .key file   1858  jan/19/2019 04:15:42
8  cert_export_Client.crt       .crt file   1164  jan/19/2019 04:15:55
9  cert_export_Client.key       .key file   1858  jan/19/2019 04:15:55
```

Let's Encrypt certificates

RouterOS v7 has Let's Encrypt (letsencrypt) certificate support for 'www-ssl' service. To enable the Let's Encrypt certificate service with automatic certificate renewal, use 'enable-ssl-certificate' command:

```
/certificate enable-ssl-certificate dns-name=my.domain.com
```

Note that the DNS name must point to the router and port TCP/80 must be available from the WAN. If dns-name is not specified, it will default to the automatically generated *ip cloud* name (ie. http://example.sn.mynetname.net)