FAQ - Generate own keys/certificates

Certificate authority:

Certificate authority example

```
openssl req -new -x509 -days 365 -extensions v3_ca -keyout ca.key -out ca.crt

Generating a RSA private key ..+++++

..................+++++

writing new private key to 'ca.key'

Enter PEM pass phrase: Gigaset123+

Verifying - Enter PEM pass phrase: Gigaset123+

-----

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:DE

State or Province Name (full name) [Some-State]:NR

Locality Name (eg, city) []:Bocholt

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gigaset

Organizational Unit Name (eg, section) []:

Common Name (e.g. server FQDN or YOUR name) []:gigaset.com

Email Address []:
```

Client certificate and key:

Client key generation (without a password)

```
openssl genrsa -out client.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)

.........................................................................+++++

...........+++++

e is 65537 (0x010001)
```

Client certificate request signing generation

```
openssl req -out client.csr -key client.key -new

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:DE

State or Province Name (full name) [Some-State]:NR

Locality Name (eg, city) []:Bocholt

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gigaset

Organizational Unit Name (eg, section) []:

Common Name (e.g. server FQDN or YOUR name) []:myCN (This must be an other Common Name then used
above, else connection will fail)

Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []: /Can be Left empty/

An optional company name []:
```

Passing the Certificate Signing Request (csr) file to our validation authority to get client certificate

Passing the Certificate Signing Request (csr) file to our validation authority to get client certificate

```
openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt -days 100

Signature ok

subject=C = DE, ST = NR, L = Bocholt, O = Gigaset, OU = myCN

Getting CA Private Key

Enter pass phrase for ca.key:Gigaset123+
```

Example 1 via Linux PC

```
mosquitto_pub --cafile GigasetCA.pem --cert client.crt --key client.key -p 8885 -h Einstein2 -u as1 -P 123456789012345678901234567890ab -t 'as1/msg/xxl/msgsrv/req/setMsg' -m '{"msgId":"1","payload":{"amsgId":"23642","sip_id":"1013","msg":{"server_msg_status":"new","prio":"1","title":{"text":"Message prio 1","color":"04"},"status_icon":"0D","status_text":"accept","ttl":"600","alert_info":"msg_melody_low","overrule_silencing":"no","vibration":"no","ringtone_volume":"50","deletable":"yes","local_ignore":"yes","presentation_time":"30","body_starter":"Body starter","msg_icon":{"value":"28"},"body":[{"msg_icon":{"value":"4E","color":"04"}},{"paragraph":{"text":"Prio 1 message: some longer test to check how long the message can be","blink":"no","underline":"yes","bold":"yes","align":"left","color":"00"}},{"paragraph":{"text":"This text is only shown in detailed view","blink":"no","underline":"no","bold":"no","align":"left"}}],"reply_options":[{"option_id":"1","reply":{"text":"Msg1SK1"}},{"option_id":"2","reply":{"text":"Msg1SK2"}},{"option_id":"3","make_call":{"text":"Call","to":"1021"}}]}}}'
```

Einstein2 is Common name in Client certificate and must be in hosts file.