FAQ - Client certificates

Valid for:	N610	N670	N870	N870E	Embedded Integrator	Virtual Integrator

Valid for N610 / N670 / N870 / N870E.

Default, Client certificates are pre-installed on the device.

The Factory installed Client certificates can be found here:

```
/config/ssl/gigaset_factory_cert.pem
/config/ssl/gigaset_factory_key.pem
```

How to check the CN:

There are 2 types of client certificates possible:

- CN = Einstein2
- CN = <MAC address> of the device example: CN = 7C2F80C6E5C2

The correct client certificate will have CN = <MAC address>

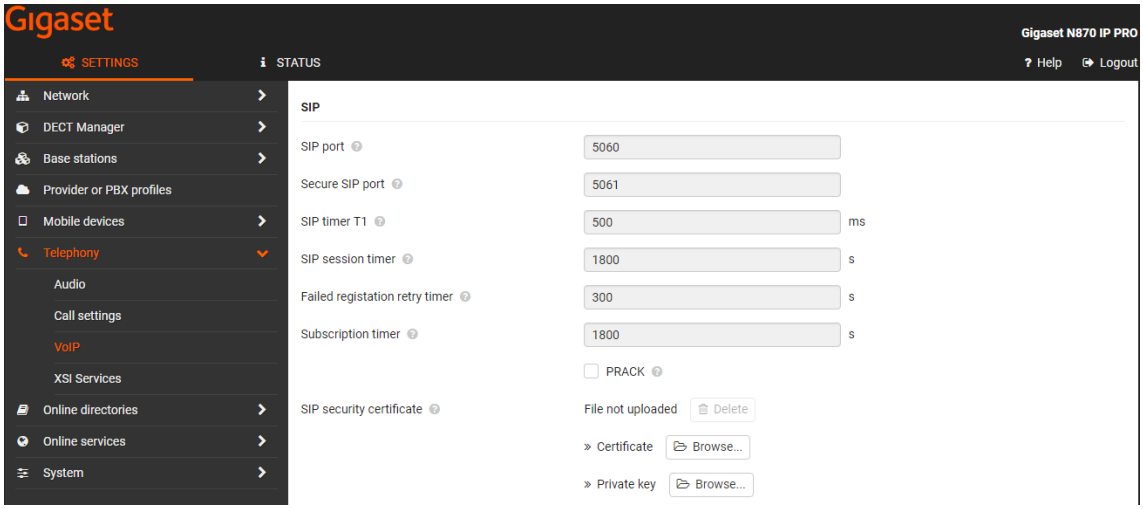
You can the check the CN using the following openssl command. You can execute this on the Nx70 (CLI access) or on external Linux PC, replace IP address with the IP address of your DECT device)

```
openssl s_client -showcerts -connect 192.168.178.192:5061 2>/dev/null | grep -A3 "Server certificate"

Server certificate
subject=C = DE, ST = DE, L = Bocholt, O = Gigaset Communications GmbH, OU = PRO, CN = Einstein2

issuer=C = DE, ST = Germany, L = Bocholt, O = Gigaset Communications GmbH, OU = Certificate Authority, CN =
Gigaset.net

Other example:

openssl s_client -showcerts -connect 192.168.178.190:5061 2>/dev/null | grep -A3 "Server certificate"

Server certificate
subject=C = DE, ST = Germany, L = Bocholt, O = Gigaset Communications GmbH, CN = 7C2F80C6E5C2

issuer=C = DE, ST = Germany, L = Bocholt, O = Gigaset Communications GmbH, OU = Certificate Authority, CN =
Gigaset.net
```

If you have an certificate with CN=Einstein2 and would need a new certificate, you can request this from Gigaset support.

Web-interface

The Client certificates can be uploaded from the web-interface, go to: **SETTINGS - Telephony - VoIP**.



Auto-provisioning

```
<?xml version="1.0" encoding="UTF-8"?>
<provisioning version="1.1" productID="e2">

<firmware>

</firmware>

<nvm>

</nvm>

<custom>

        <step type="certificate" url="<URL to certificate>" key="<URL to Private key>" flags="CLIENT_CERT" />

</custom>

</provisioning>
```

How to generate Client certificates

You can generate your own Client certificates using a Linux machine.

To create self-signed client certificate you have to follow the instructions below. If you have own CA you can skip the first step.
1. Generate CA certificate (ca.crt) and key (ca.key):

```
openssl genrsa -des3 -out ca.key 4096
openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

and follow the on-screen instructions.

2. Generate Client Key, Certificate Signing Request, and Signed Client Certificate:

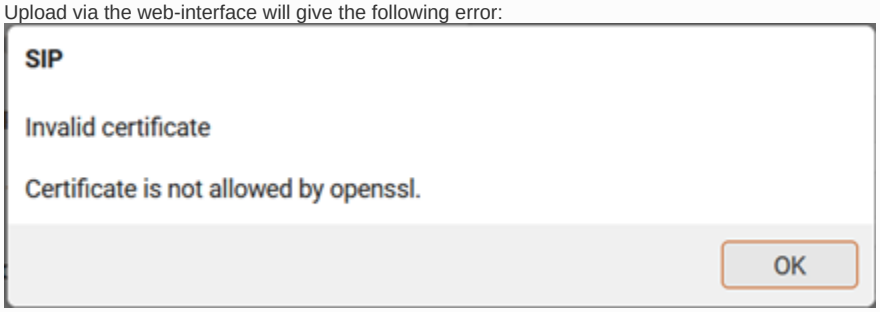
```
openssl genrsa -des3 -out N870.key 4096
openssl req -new -key N870.key -out N870.csr
openssl x509 -req -days 365 -in N870.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out N870.crt
openssl rsa -in N870.key -out N870_key.pem
```

3. To check the content of the certificate:

```
openssl x509 -in N870.crt -text -noout

Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
....
```

If you use an older Linux version, SHA1 is used by default. SHA1 is not seen as secure any-more and since software 2.57 SHA1 certificates are not accepted any-more.

Upload via the web-interface will give the following error:



In the above example, sha256 is used and is seen as secure.

As Common Name you can put the MAC address of the device (with capital letters).

You can download the **N870.crt** and **N870_key.pem** file using WinSCP.

Go to: **SETTINGS - Telephony - VoIP** to upload **N870.crt** and **N870_key.pem** files.