

FAQ - Application server connection examples Certificates

Introduction

On this page we would like to show some connection examples using Certificates and error descriptions.

Set-up:

- Nx70 software 2.44.0
- DECT handset R700H software release 11
- ...

Configuration:

1. The Application server must be enabled [FAQ - Application servers](#)
2. Messaging and Location enabled for the handset [FAQ - Messaging and Location how to enable/disable per handset](#)
3. How to generate your own security keys and certificates [FAQ - Generate own keys/certificates](#)
4. Upload ca.crt into your Nx70 [FAQ - Upload ca.crt](#)
5. Contact Gigaset to get the GigasetCA.pem that is needed on the server where mosquitto is executed [FAQ - GigasetCA.pem \(Hidden\)](#)
6. Add device to the known hosts [FAQ - Add device to the known hosts](#)

Example of publish for getting basic information from system

```
mosquitto_pub --cafile GigasetCA.pem --cert client.crt --key client.key -m '{"msgId":"1234","params":{}}' -t "as1/module/xxl/api/req/status" -p 8885 -h Einstein2 -u as1 -P 123456789012345678901234567890ab
```

MQTT message example:

- Prio 1 message
- To handset with SIP ID 1014
- With "Fire" icon and some text

MQTT example using Linux PC

Nx70 has no config/ssl directory so we used the **Einstein2** hostname as the Client certificate in the Nx70 CN=Einstein2

Mosquitto version 1.4.15

```
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":{"amsId":"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","override_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"}}}}}}'
```

MQTT example using Linux PC

Nx70 has no config/ssl directory so we used the **Einstein2** hostname as the Client certificate in the Nx70 CN=Einstein2

mosquitto version 2.0.11 (add "-i as1")

```
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":{"amsId":"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","override_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"}}}}}}' -i as1
```

MQTT example 2 using Linux PC

We have uploaded a new Client certificate:

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number:
    f6:7a:af:8c:03:e7:3d:ed
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=DE, ST=Germany, L=Bocholt, O=Gigaset Communications GmbH, OU=Certificate Authority, CN=Gigaset.net
Validity
    Not Before: Dec  6 11:19:04 2018 GMT
    Not After : Jun  6 11:19:04 2030 GMT
Subject: C=DE, ST=Germany, L=Bocholt, O=Gigaset Communications GmbH, CN=7C2F80F68993
Subject Public Key Info:
```

CN = 7C2F80F68993

Then we need to change the hosts file and add the device to the host file:

192.168.178.195 7C2F80F68993

The MQTT command will now use the MAC address instead of Einstein2

```
mosquitto_pub --cafile GigasetCA.pem --cert client.crt --key client.key -p 8885 -h 7C2F80F68993 -u as1 -P
123456789012345678901234567890ab -t 'as1/msg/xxl/msgsrv/req/setMsg' -m '{"msgId":"1","payload":{"amsId":"23642","sip_id":"1014","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","override_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"}}}}}'
```

MQTT example 2 using Windows PC

Windows: mosquitto version 2.0.14

Nx70: Software 2.44.0

```
.\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\:{\amsId:\23642\,\sip_id:\1013\,\msg\:{\server_msg_status\:\new\,\
prio\:\1\,\title\:{\text\:\Message prio1\,\color\:\04\},
\status_icon\:\0D\,\status_text\:\accept\,
\ttl\:\600\,
\alert_infol\:\msg_melody_low\,
\override_silencing\:\no\,
\vibration\:\no\,
\ringtone_volume\:\50\,
\presentation_time\:\30\,
\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\}}}}' -i as1
```

Windows: mosquito version 2.0.15

```

./mosquitto_pub --cafile GigasetCA.pem --cert client.crt --key client.key -p 8885 -u as1 -P 123456789012345678901234567890ab -t
'as1/msg/xxl/msgsrv/req/setMsg' -m "{\n  \"msgId\": \"11\", \"payload\": {\n    \"amsgId\": \"23642\", \"sip_id\": \"1013\", \"msgl\": {\n      \"server_msg_status\": \"new\", \"prio\": \"11\", \"title\": {\n        \"text\": \"Message prio1\", \"color\": \"04\"}, \"status_icon\": \"0D\", \"status_text\": \"accept\", \"ttl\": \"600\", \"alert_info\": {\n      \"msg_melody_low\", \"override_silencing\": \"no\", \"vibration\": \"no\", \"ringtone_volume\": \"50\", \"presentation_time\": \"30\", \"deletable\": \"yes\", \"local_ignore\": \"yes\", \"presentation_time\": \"30\", \"body_starter\": \"Body starter\", \"msg_icon\": {\n      \"value\": \"28\", \"body\": {\n        \"msg_icon\": {\n          \"value\": \"4E\", \"color\": \"04\"}, {\n          \"paragraph\": {\n            \"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\"}, {\n            \"paragraph\": {\n              \"text\": \"This text is only shown in detailed view\", \"blink\": \"no\", \"underline\": \"no\", \"bold\": \"no\", \"align\": \"left\"}, {\n            \"reply_options\": {\n              \"option_id\": \"11\", \"reply\": {\n                \"text\": \"Msg1SK1\"}, {\n              \"option_id\": \"21\", \"reply\": {\n                \"text\": \"Msg1SK2\"}, {\n              \"option_id\": \"31\", \"make_call\": {\n                \"text\": \"Call\", \"to\": \"1021\"}}}}}} -i as1

```