



How to use TLS in MyPBX

Version: V1.0

Date: August, 2013

Yeastar Information Technology Co. Ltd

Content

- Introduction..... 3
- 1. How to register IP phones to MyPBX via TLS 3
 - 1.1 ENABLE TLS IN MYPBX’S WEB INTERFACE..... 3
 - 1.2 PREPARE THE WHOLE CERTIFICATES FOR TLS 5
 - 1.3 UPLOAD CERTIFICATES 19
 - 1.4 REGISTER IP PHONE TO MYPBX VIA TLS 24
- 2. How to register SIP trunk to VoIP provider via TLS..... 27

Introduction

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

TLS is supported in MyPBX for security SIP registry; you can also register SIP trunks to VoIP providers via TLS. We need upload the certificate into MyPBX and the IP phones together for authorization.

Note: TLS is disabled in MyPBX by default; we need enable it in 'SIP settings' page in advance before use it.

1. How to register IP phones to MyPBX via TLS

MyPBX is working as a SIP server, IP phones register to MyPBX as an extension via TLS.

1.1 Enable TLS in MyPBX's web interface

Click 'PBX→SIP settings→General' to get the settings about TLS, which is disabled by default. If you are using MyPBX standard, please find it in 'Internal settings→SIP settings' page.

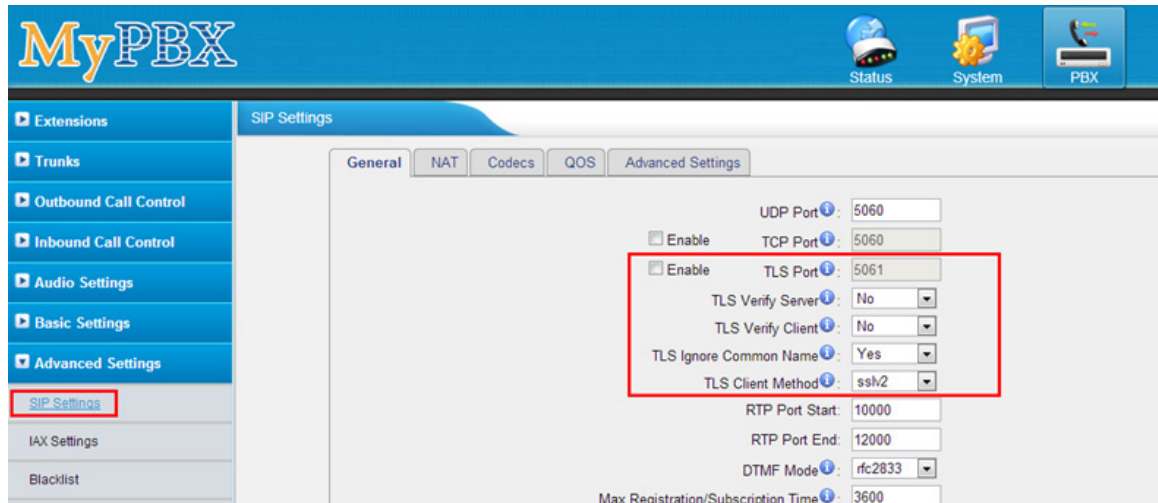


Figure 1-1

•TLS Port

Port use for sip registrations, Default is 5061.

•TLS Verify Server

When using MyPBX as a TLS client, whether or not to verify server's certificate. It is "No" by default.

•TLS Verify Client

When using MyPBX as a TLS server, whether or not to verify client's certificate. It is "No" by default.

•TLS Ignore Common Name

Set this parameter as "No", then common name must be the same with IP or domain name.

•TLS Client Method

When using MyPBX as TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.



Figure 1-2

Note:

1. For top security, we recommend to enable 'TLS Verify Client', disable 'TLS Ignore Common Name', MyPBX will verify IP phone's Certificate, the common name inside CA should be the same as its IP or domain name.
2. TLS Client Method, it's the TLS method of IP phone, you can contact the manufactory of IP phone to get that.
3. You need reboot MyPBX to take effect after enable TLS.

1.2 Prepare the whole certificates for TLS

Here are the whole certificates of MyPBX and IP phones for TLS registry as the screen shot above:

MyPBX's CA: CA.crt.

MyPBX's server certificate: asterisk.pem.

IP phone's CA: CA.crt or CA.csr.

IP phone's server certificate: client.pem.

The certificate is generated via the toolkit of openssl, you can compile the source package from <http://www.openssl.org/>, or download the tool I used here, download link:

www.yeastar.com/download/tools/TLS_CA_Tool.rar

You can find the files inside the package like these:

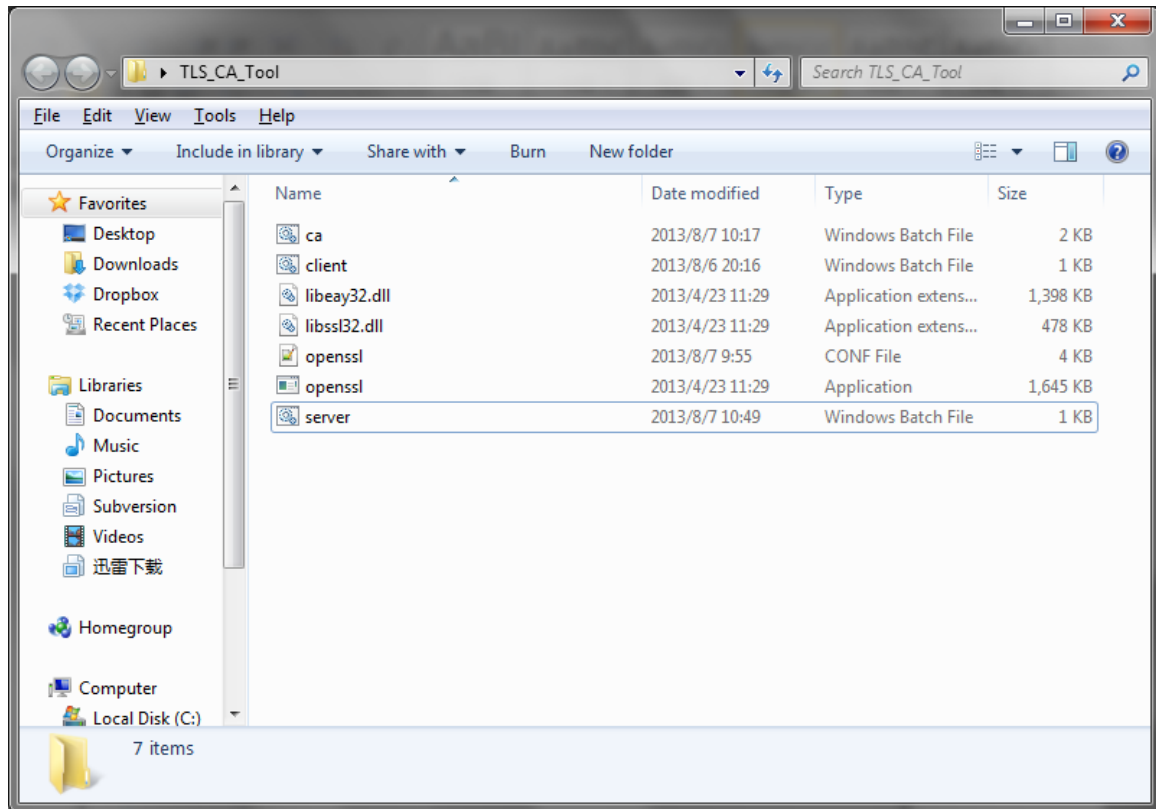


Figure 1-3

Ca.bat: Make the CA.crt for IP phone and MyPBX

Client.bat: make the 'client.pem', it's the 'IP phone's server certificate'.

Server.bat: make the 'asterisk.pem', it's the 'MyPBX's server certificate'.

Here are the steps to make the whole certificates.

Step1. Prepare MyPBX's CA: CA.crt

Double click ca.bat

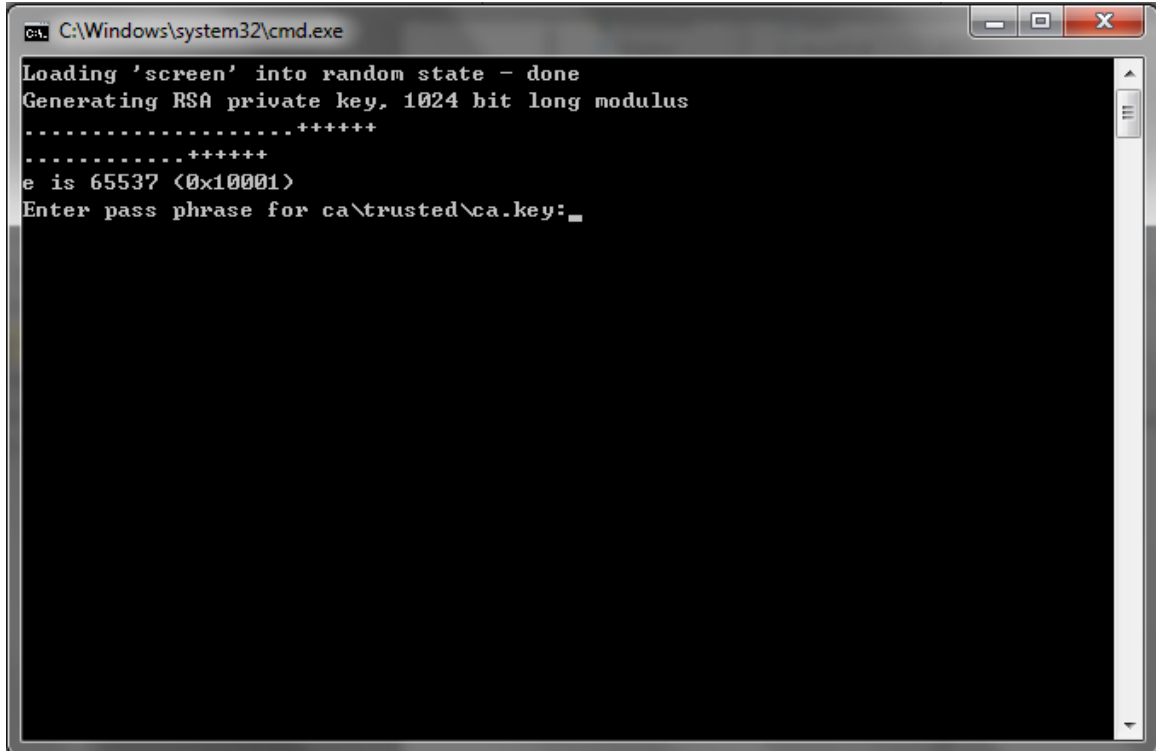


Figure 1-4

Just follow the guide to input the information of MyPBX step by step, In this example, MyPBX's IP address is 192.168.4.142.

```
C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
..+++++
e is 65537 (0x10001)
Enter pass phrase for ca\trusted\ca.key:
Verifying - Enter pass phrase for ca\trusted\ca.key:
Enter pass phrase for ca\trusted\ca.key:
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) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, ip address, website) [192.168.4.142]
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=Some-State/O=Internet Widgits Pty Ltd/CN=192.168.4.142
Getting Private key
Enter pass phrase for ca\trusted\ca.key: _
```

Figure 1-5

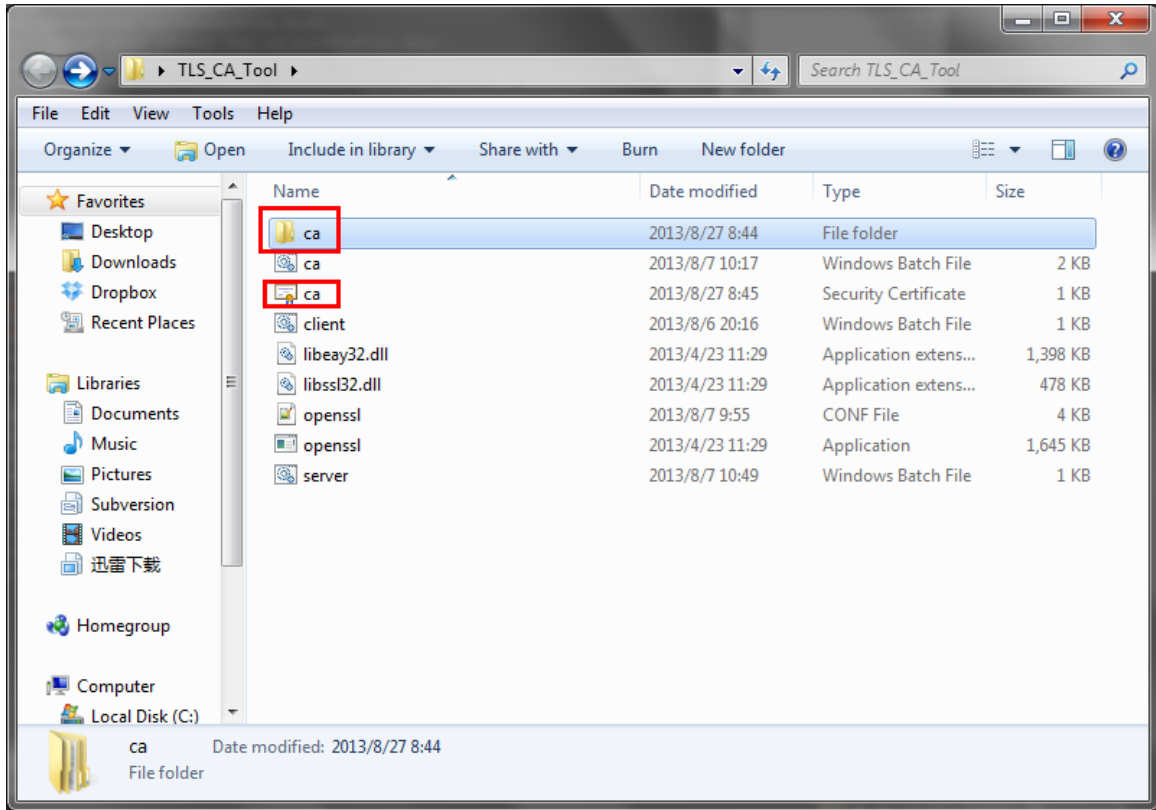


Figure 1-6

This ca.crt is the same as the one in folder /TLS_CA_Tool/ca/trusted/.

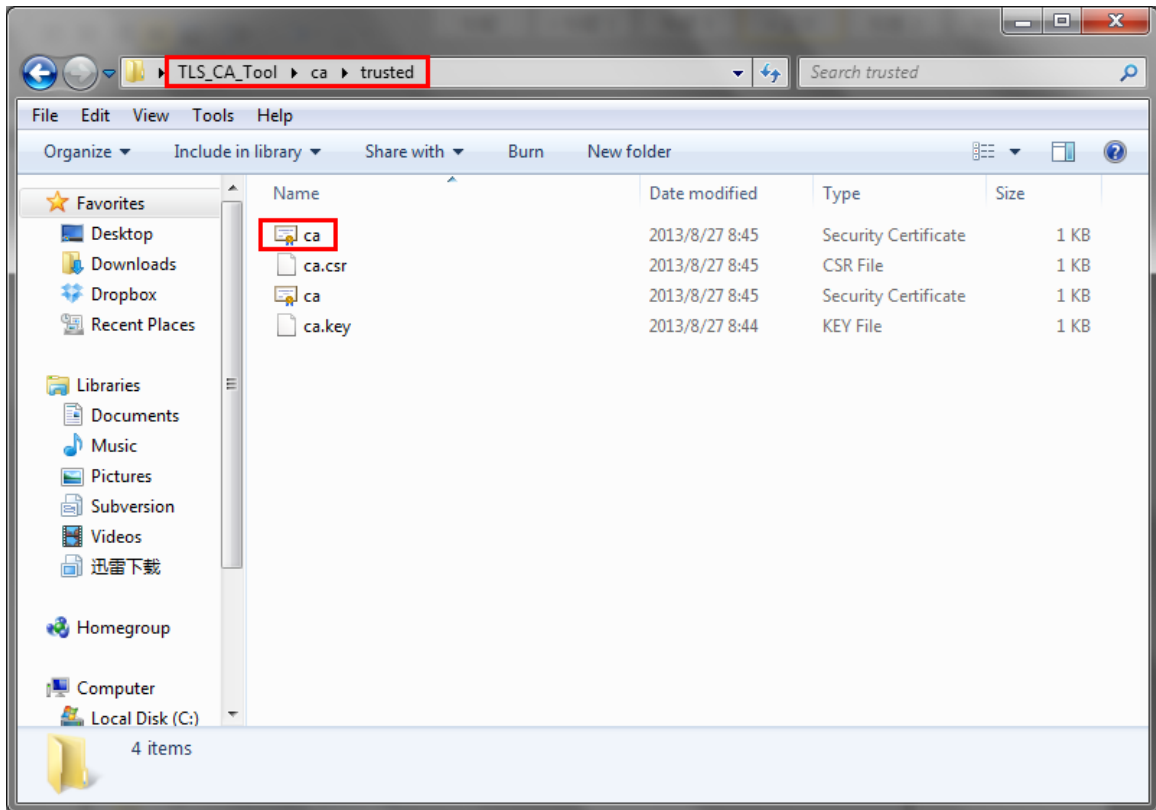


Figure 1-7

MyPBX's CA: CA.crt is generated successfully.

Step2 Prepare 'asterisk.pem', 'MyPBX's server certificate'

We need the CA.crt and CA.key to make the server certificate.
Double click 'server.bat'.

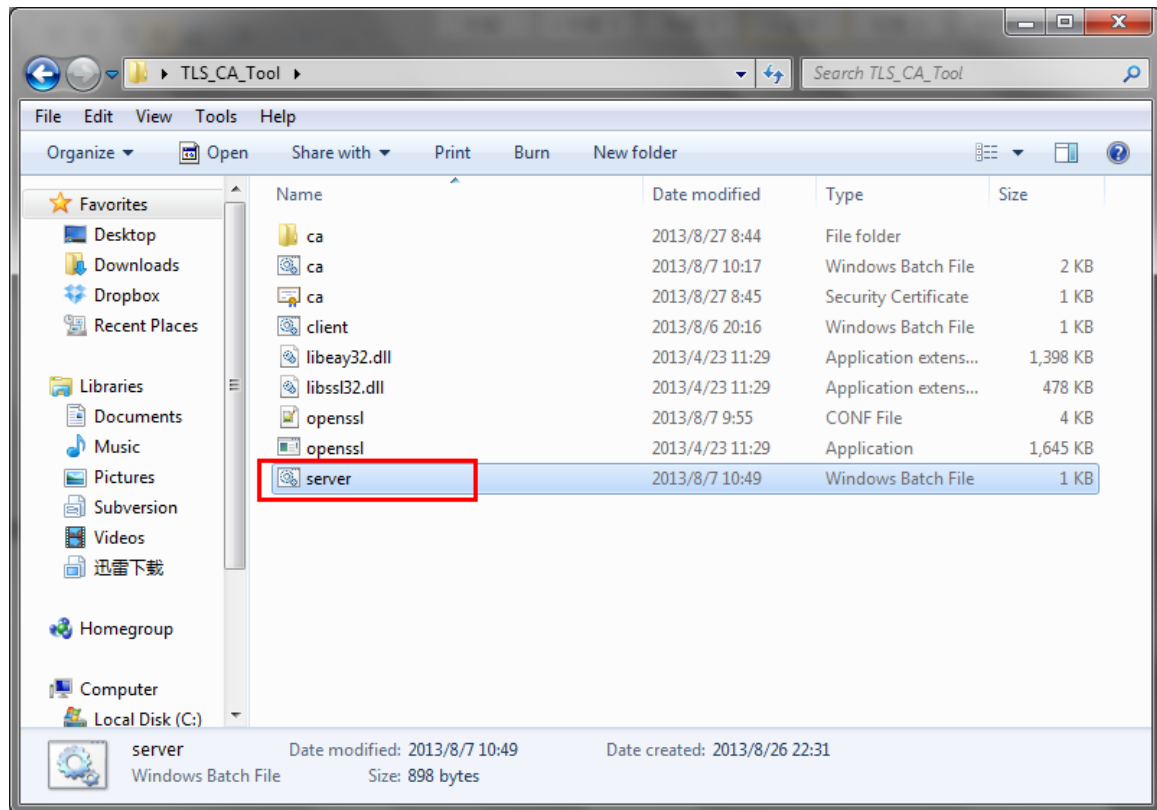


Figure 1-8

Follow the guide to input information step by step, and make sure the information you have input matches the one you have input in step1.

```
C:\Windows\system32\cmd.exe
Could Not Find C:\Users\Harry\Desktop\TLS_CA_Tool\ca\serial*
Could Not Find C:\Users\Harry\Desktop\TLS_CA_Tool\ca\index.txt*
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca\server\server.key'
-----
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) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, ip address, website) [192.168.4.142]:
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'Some-State'
organizationName  :PRINTABLE:'Internet Widgits Pty Ltd'
commonName        :PRINTABLE:'192.168.4.142'
Certificate is to be certified until Aug 25 00:51:20 2023 GMT (3650 days)
Sign the certificate? [y/n]:y
```

Figure 1-9

Check the whole information then input y to continue, when done, you can find the asterisk.pem as the following picture shows.

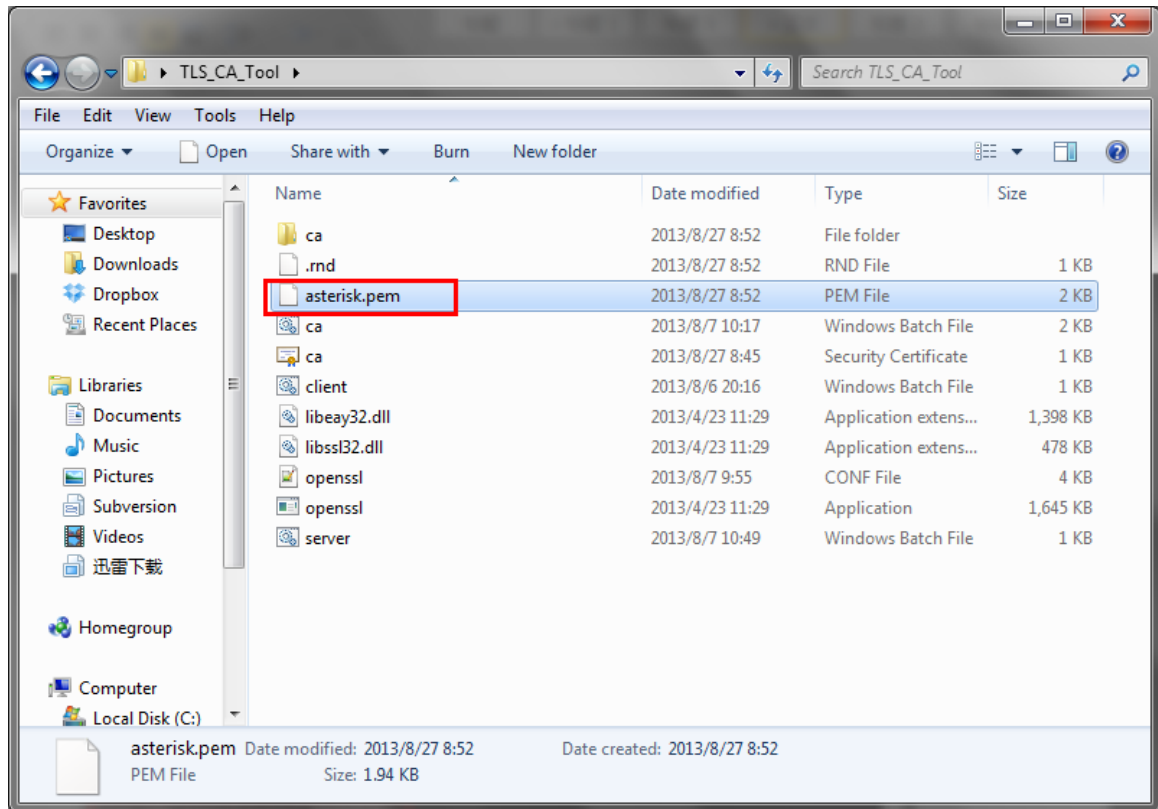


Figure 1- 10

asterisk.pem, the 'MyPBX's server certificate' is generated successfully.

Note: We can copy the asterisk.pem, ca.crt to another folder before making the IP phone's certificate.

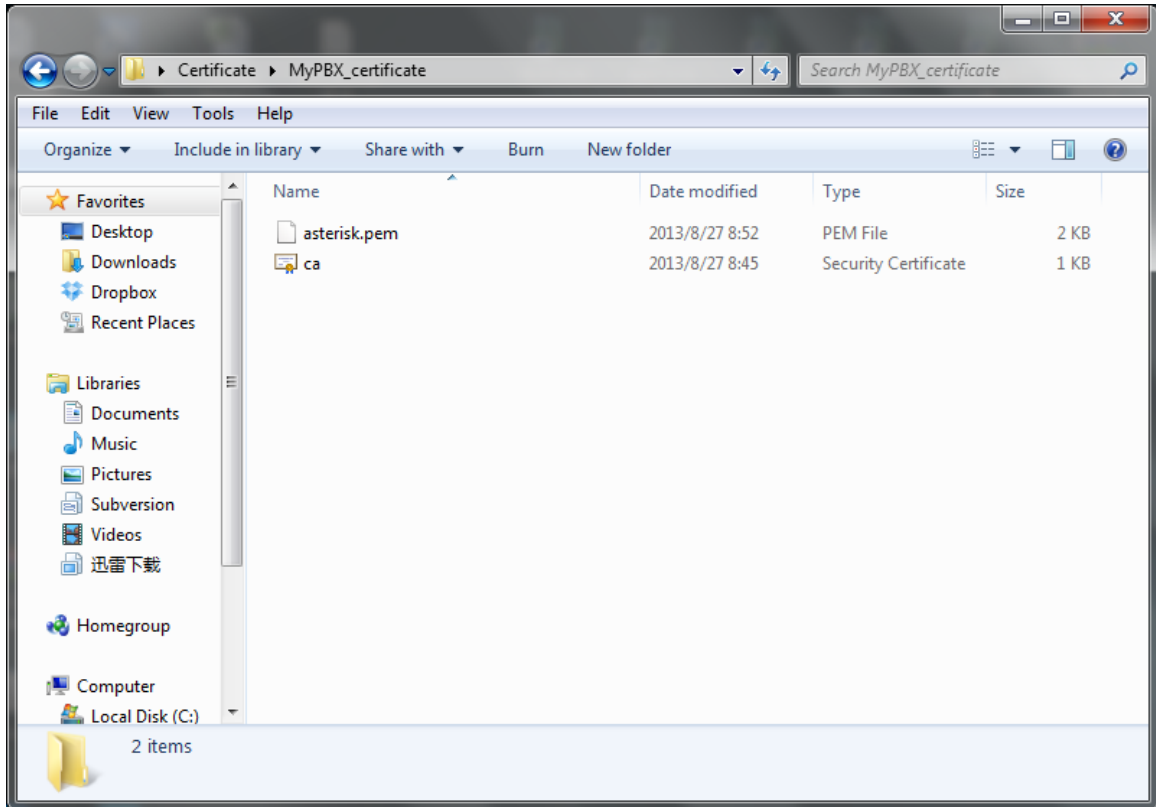


Figure 1-11

Step3. Prepare the IP phone's certificate, ca.crt

Double click 'ca.bat', input the information of IP phone step by step

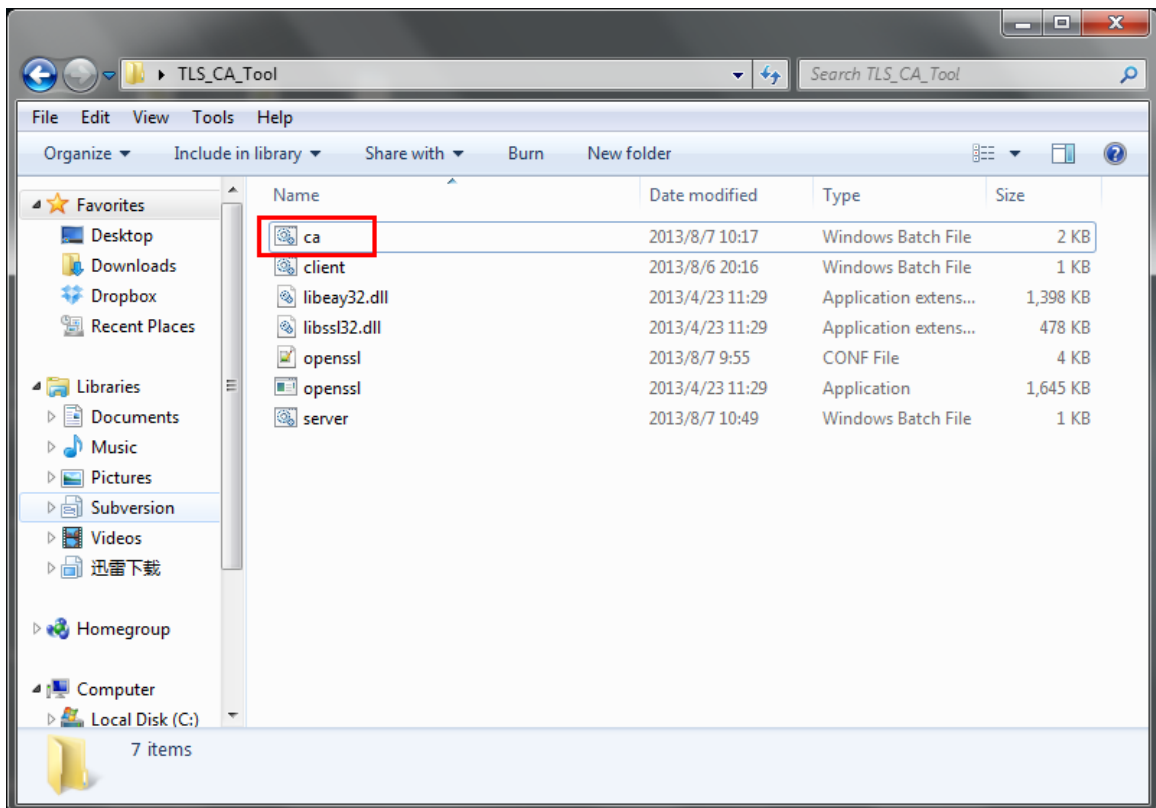
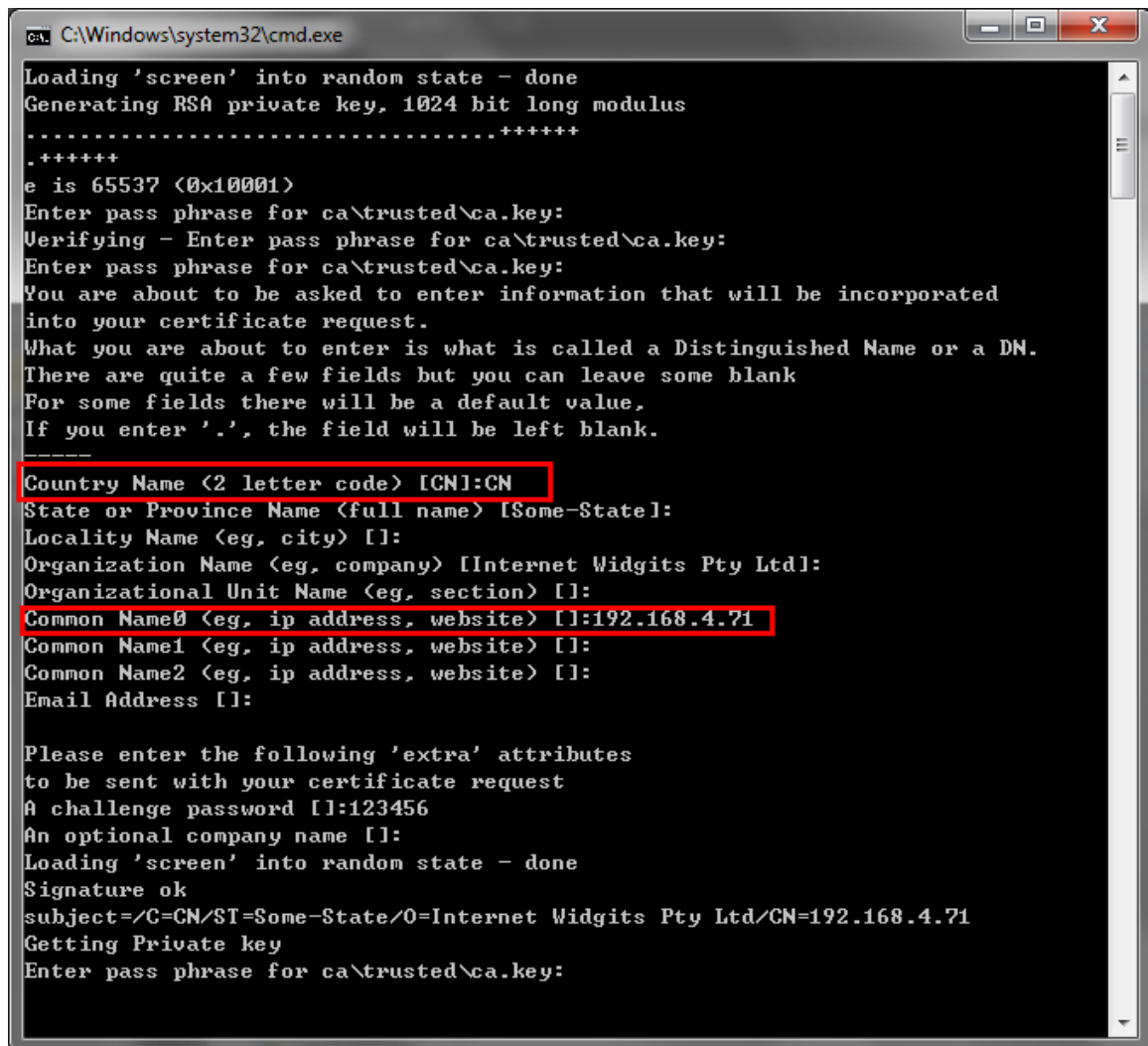


Figure 1-12

In this example, the IP phone's IP address is 192.168.4.71.



```
C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
..+++++
e is 65537 (0x10001)
Enter pass phrase for ca\trusted\ca.key:
Verifying - Enter pass phrase for ca\trusted\ca.key:
Enter pass phrase for ca\trusted\ca.key:
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) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.4.71
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=Some-State/O=Internet Widgits Pty Ltd/CN=192.168.4.71
Getting Private key
Enter pass phrase for ca\trusted\ca.key:
```

Figure 1-13

When done, we can find the ca.crt in this folder.

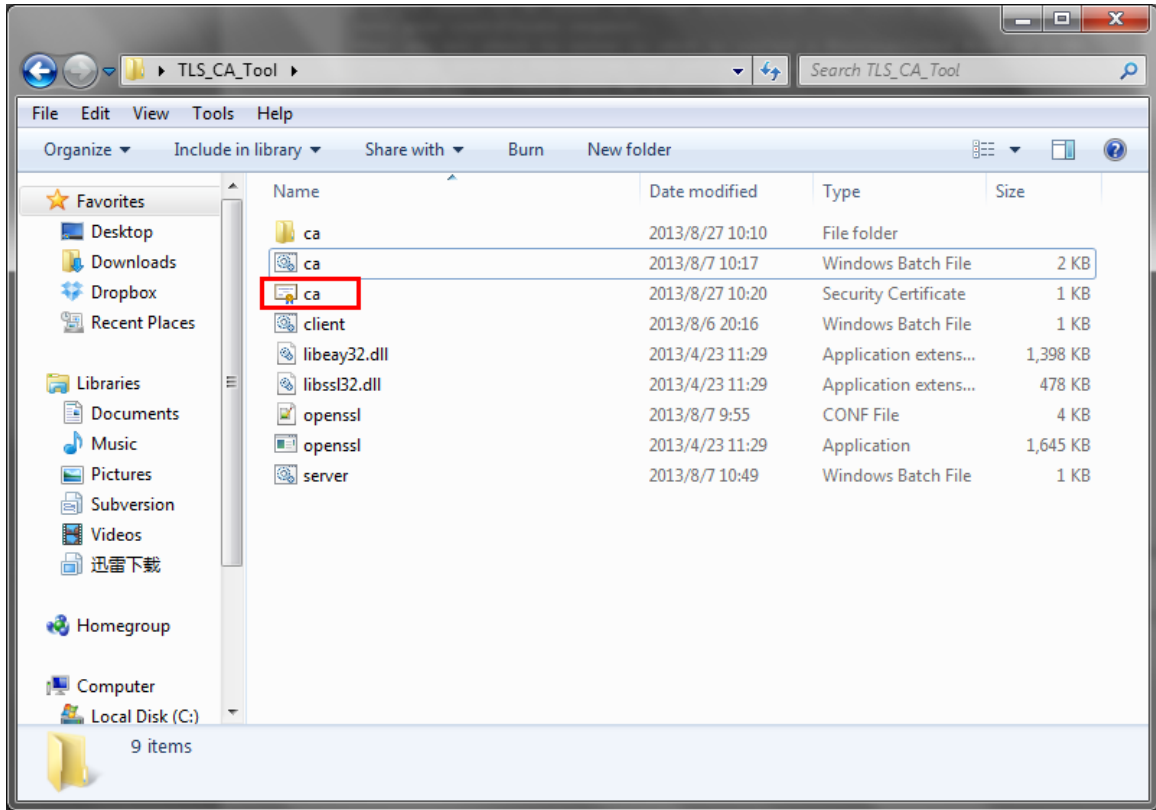


Figure 1- 14

The ca.crt in folder /TLS_CA_Tool/ca/trusted is the same as the above one.

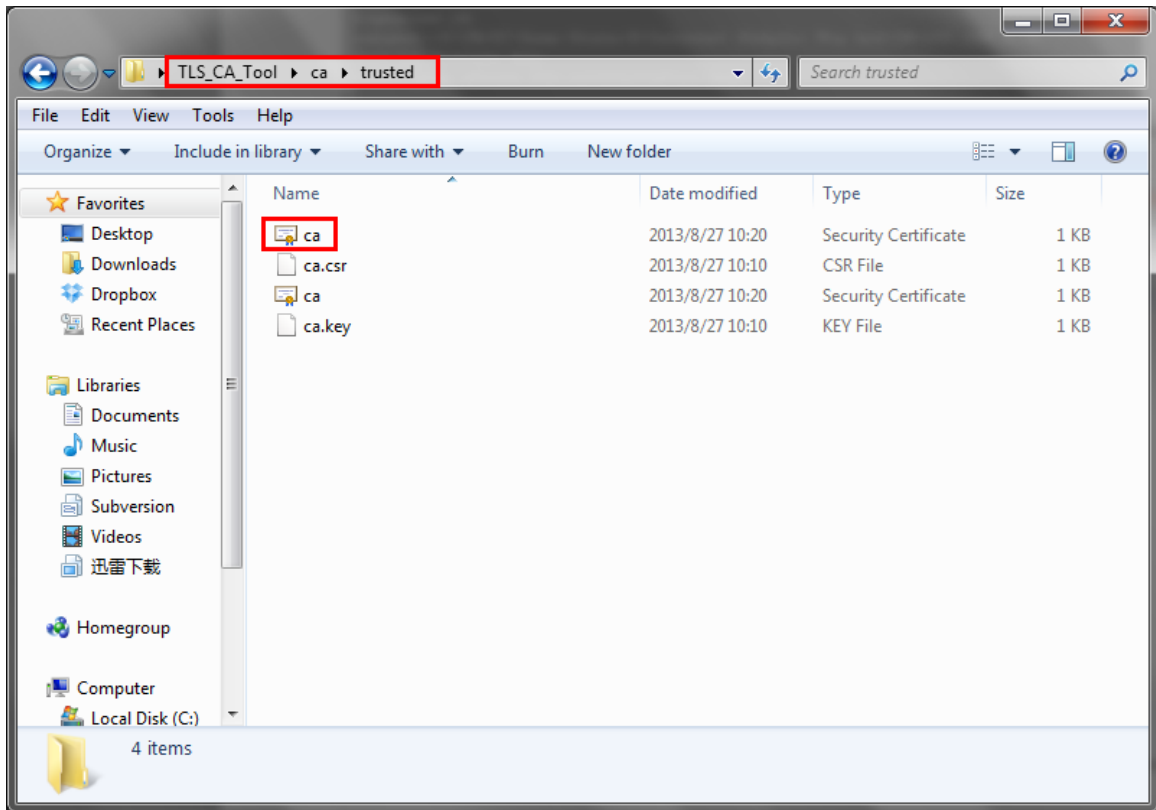


Figure 1- 15

The IP phone's certificate is finished.

Note: If you have got your own CA for IP phone, you can rename it to CA.crt and copy it to folder '/TLS_CA_Tool/ca/trusted' before making the 'client.pem'.

Step4. Prepare 'client.pem', the 'IP phone's server certificate'.

Double click 'client.bat'.

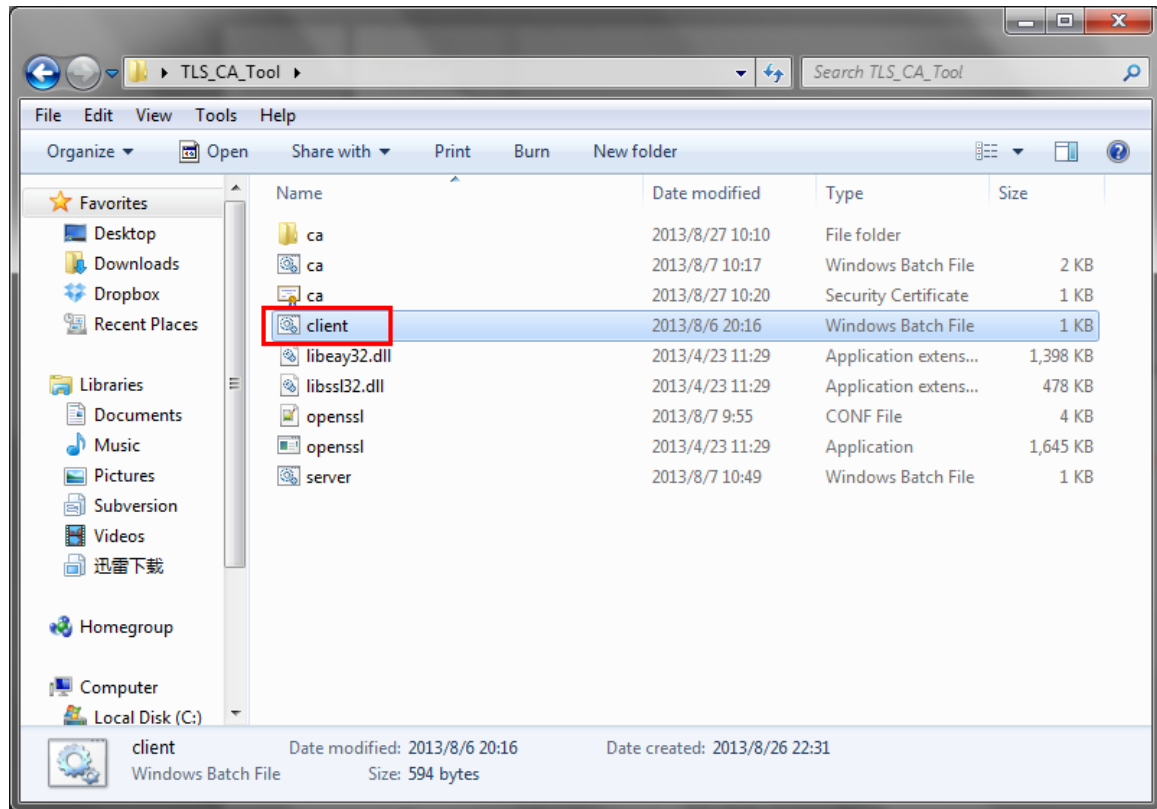


Figure 1-16

Input the IP phone's information step by step in this script; make sure the content is the same as step 3.


```
C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca\client\client.key'
-----
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> [CN]:CN
State or Province Name <full name> [Some-State]:
Locality Name <eg, city> []:
Organization Name <eg, company> [Internet Widgits Pty Ltd]:
Organizational Unit Name <eg, section> []:
Common Name0 <eg, ip address, website> []:192.168.4.71
Common Name1 <eg, ip address, website> []:
Common Name2 <eg, ip address, website> []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'Some-State'
organizationName  :PRINTABLE:'Internet Widgits Pty Ltd'
commonName        :PRINTABLE:'192.168.4.71'
Certificate is to be certified until Aug 25 02:30:44 2023 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y_
```

Figure 1-17

Confirm all the information we input before click y to finish this guide.

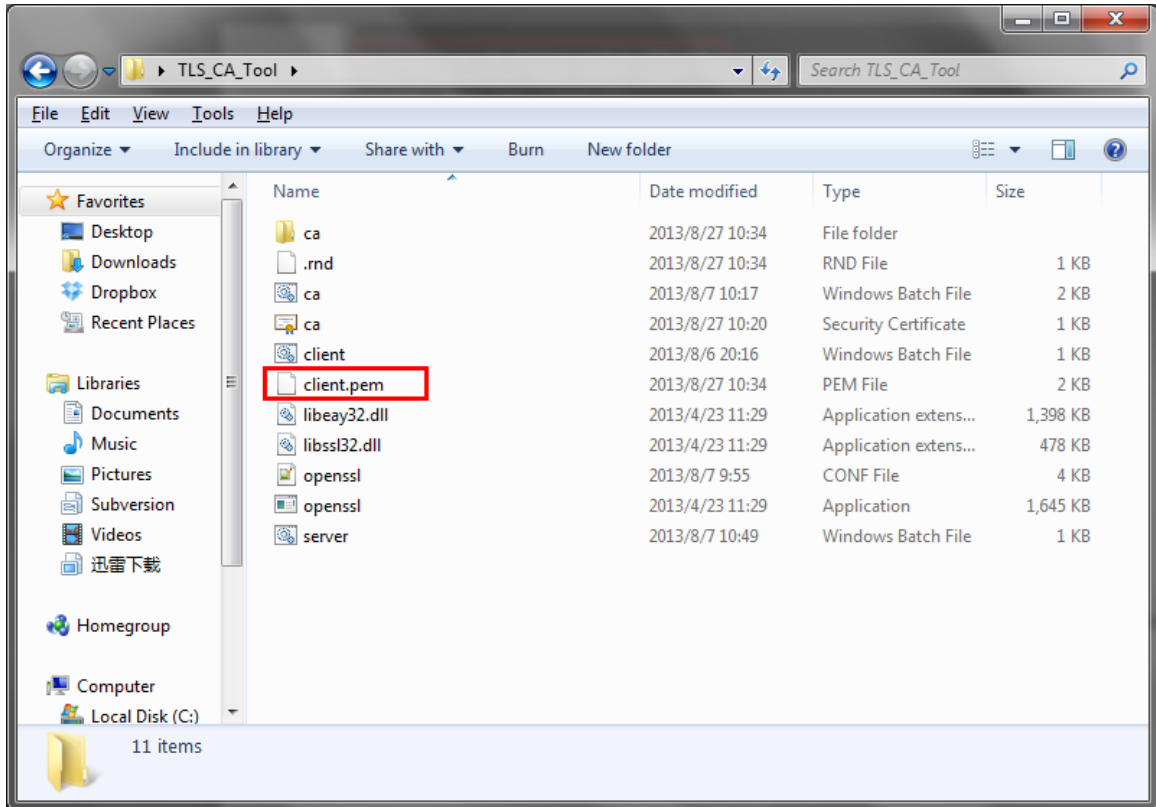


Figure 1-18

The 'IP phone's server certificate' is ready.

Note: We can copy the client.pem, ca.crt to another folder before uploading.

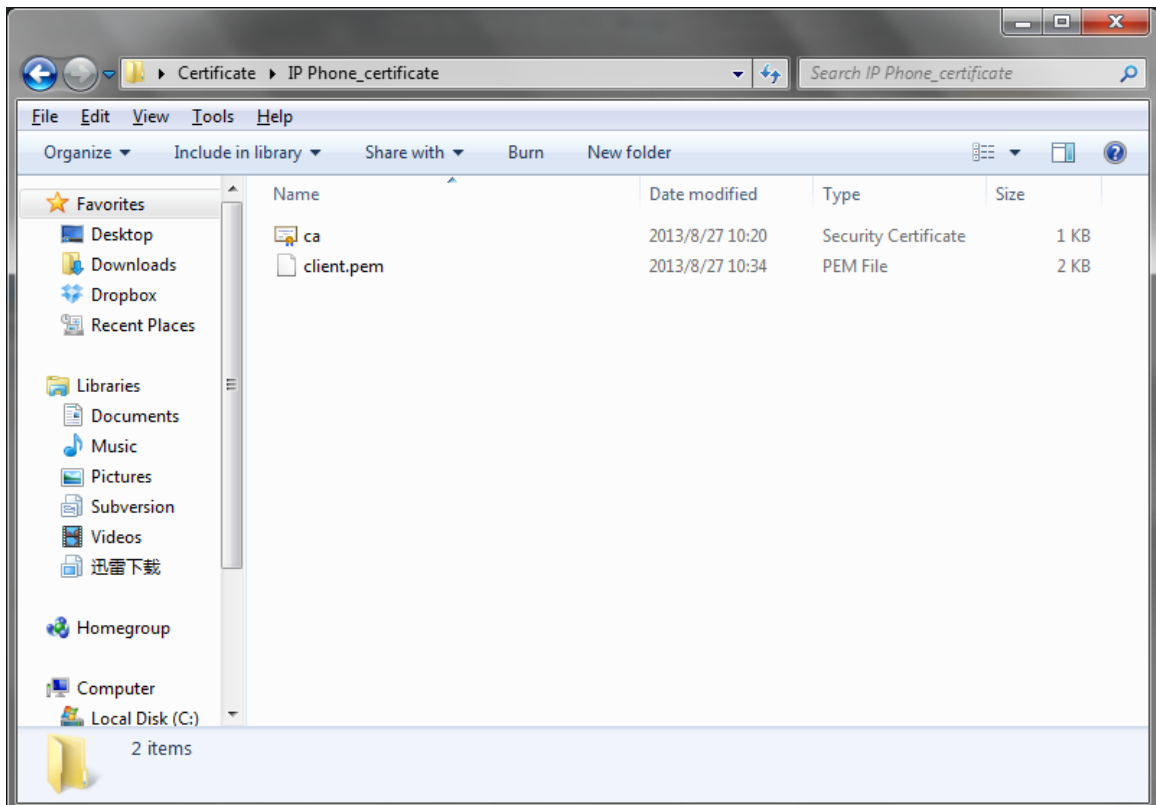


Figure 1-19

All the certificates are prepared well.

1.3 Upload certificates

1.3.1 Upload IP phone's certificates

In this example, IP phone's model is Yealink T28.

Step1. Upload 'IP phone's server certificate' (client.pem).

Click 'Security→server certificates' to upload client.pem

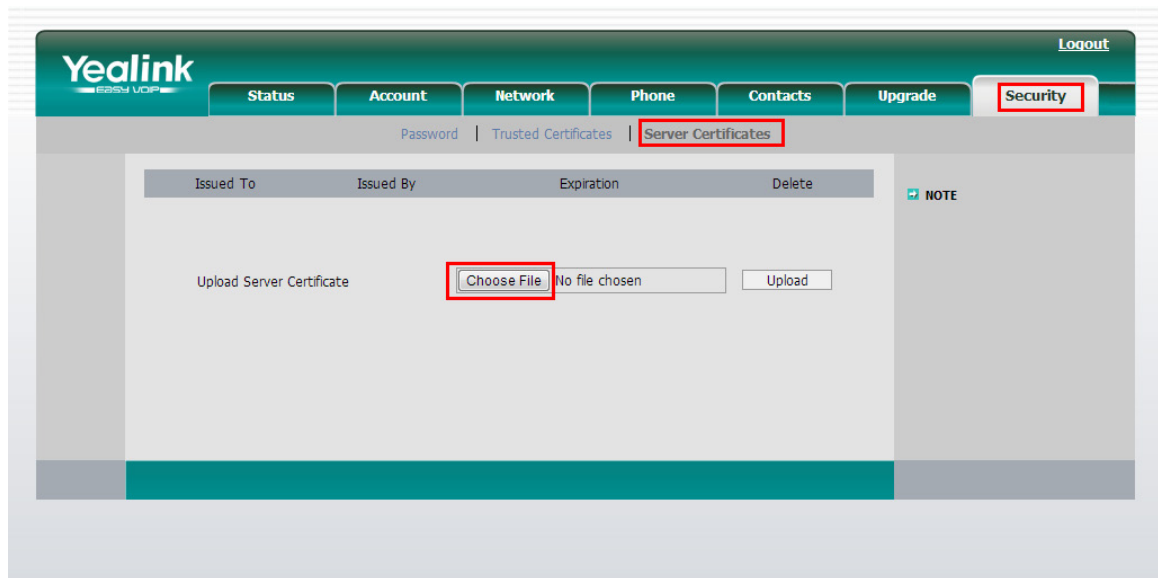


Figure 1-20

Click 'Choose File' and upload IP phone's server certificate. IP phone will reboot by itself when uploaded successfully to take effect.

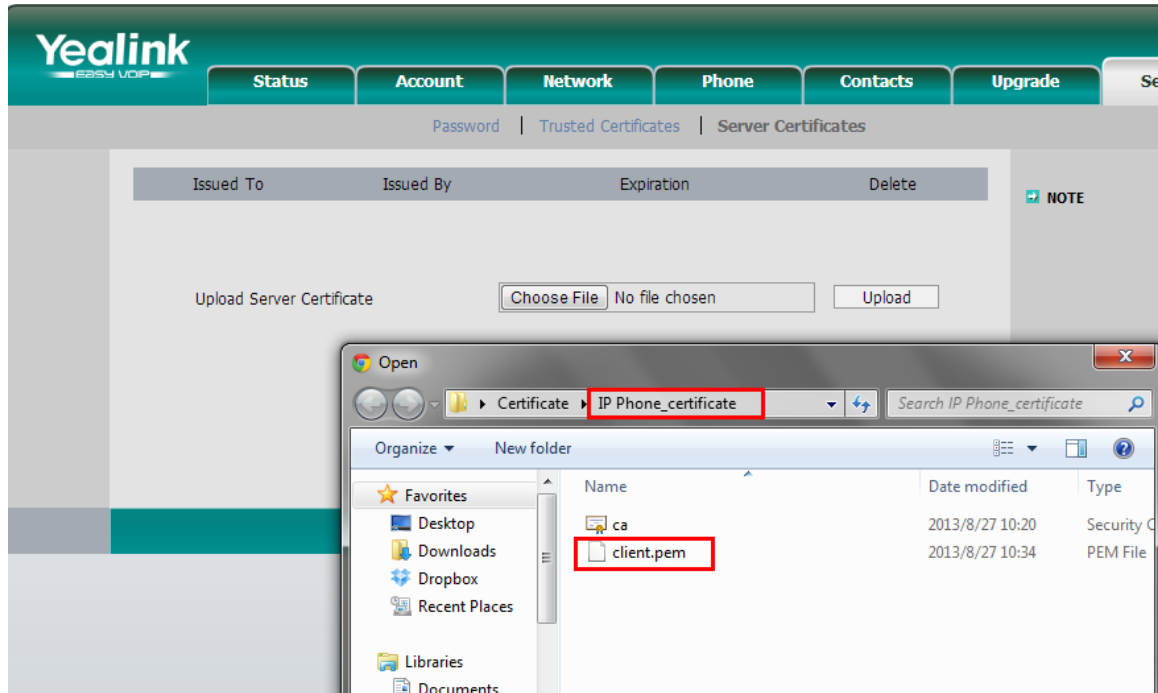


Figure 1-21

When IP phone boots up again, we can check the certificate status.

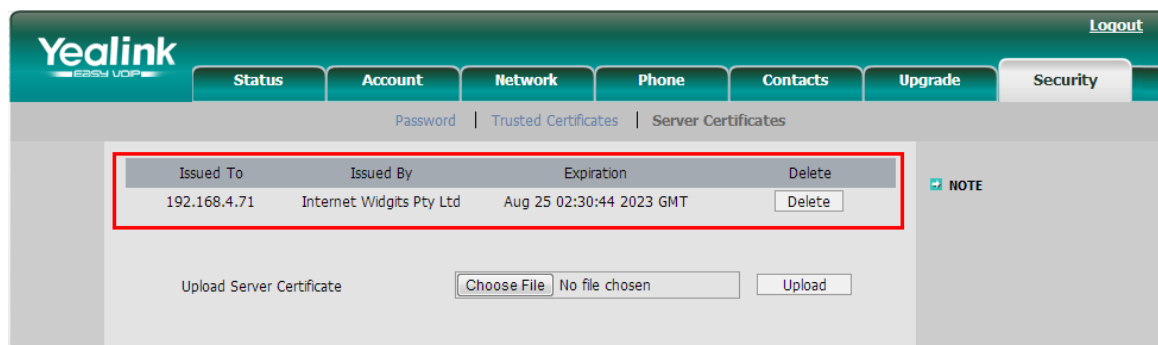


Figure 1-22

Step2. Upload the trusted certificate.

The trusted certificate is the ca.crt of MyPBX. It will send to MyPBX for during the registry process for authorization.

Click 'Security→Trusted Certificates', upload MyPBX's ca.crt.

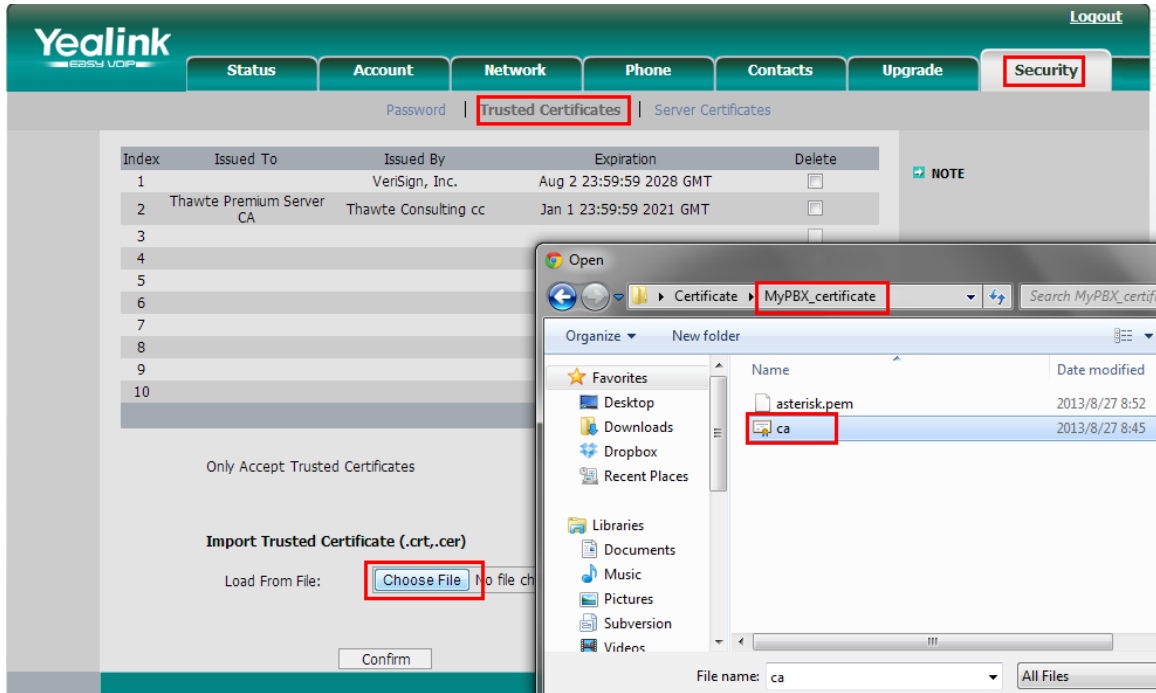


Figure 1-23

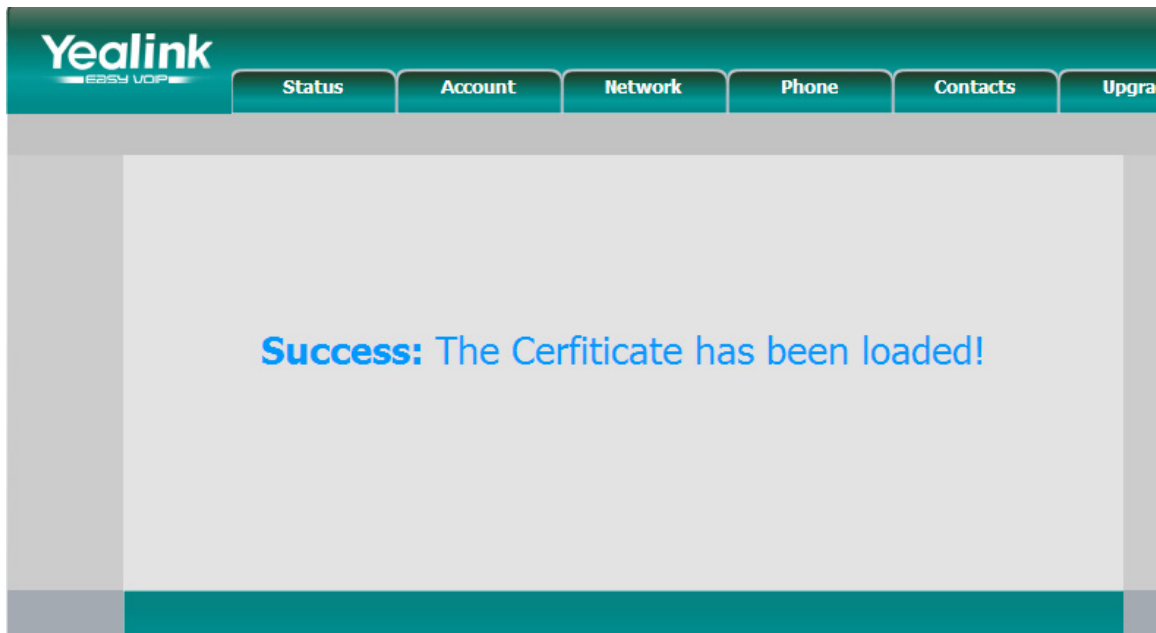


Figure 1-24

When done, we can check the content of CA.crt like the picture shows below.

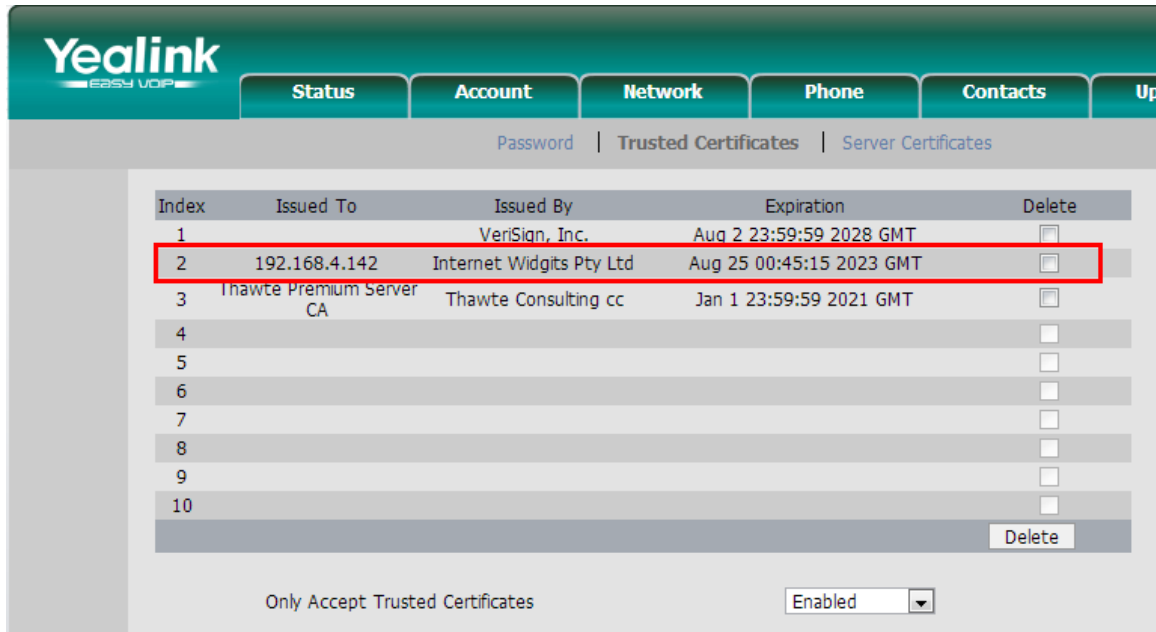


Figure 1-25

The certificates in IP phone side are uploaded well.

1.3.2 Upload MyPBX's certificates

In this example, the model of MyPBX is MyPBX U200 (firmware version: 15.18.0.22)

Step1. Upload MyPBX's server certificate (asterisk.pem)

Click 'PBX->Advanced settings->Certificates', then click 'upload certificates', choose 'PBX certificates' in Type windows, then upload the asterisk.pem.

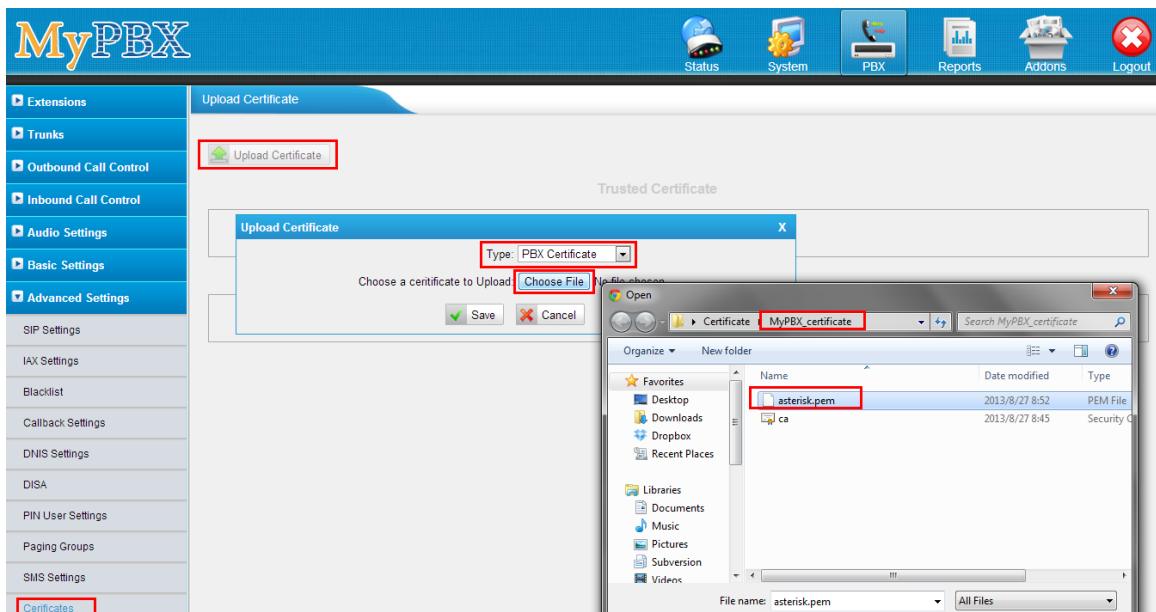


Figure 1-26

Click Save to upload, you will need to reboot MyPBX to take effect.

Upload Certificate Apply Changes

Upload Certificate

Trusted Certificate

No Certificates Defined

PBX Certificate

#	Name	Issued To	Expiration
1	asterisk.pem	192.168.4.142	Aug 25 00:51:20 2023 GMT

Reboot

Warning: Rebooting the appliance will terminate all active calls!

Reboot Now

Figure 1-27

Click 'Reboot Now' to reboot MyPBX, when done, we can continue to step 2.

Upload Certificate

Upload Certificate

Trusted Certificate

No Certificates Defined

PBX Certificate

#	Name	Issued To	Expiration
1	asterisk.pem	192.168.4.142	Aug 25 00:51:20 2023 GMT

Figure 1-28

Step2. Upload the trusted certificate.

The trusted certificate in MyPBX should be the ca.crt of IP phone.
Click 'Upload certificates' and choose 'trusted certificates' in Type windows, then upload the IP phone's ca.crt.

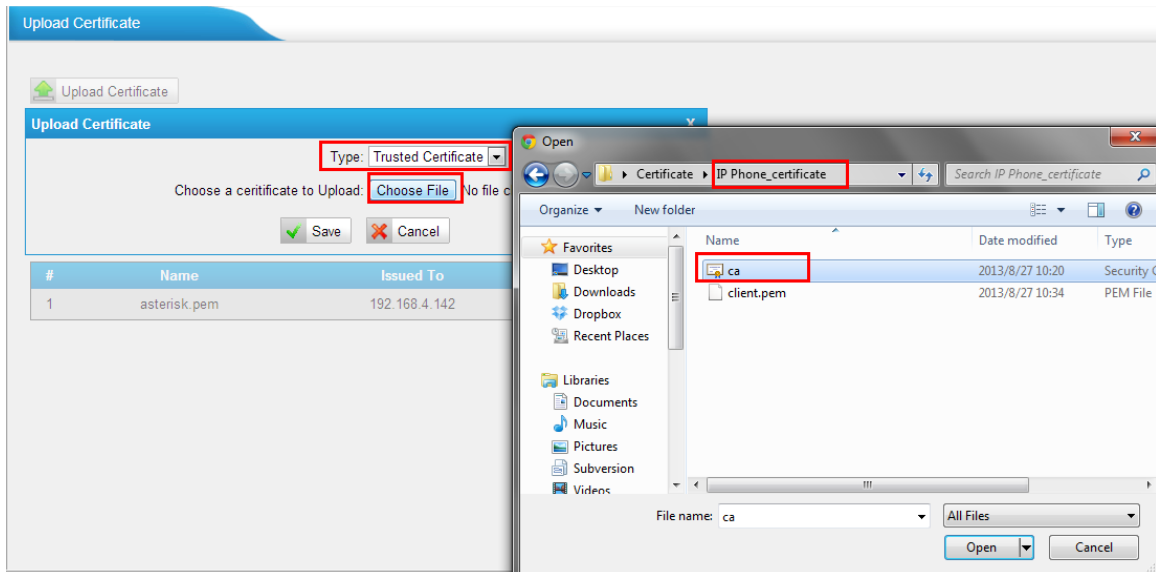


Figure 1-29

Click 'Save' to upload, then click 'apply the changes'

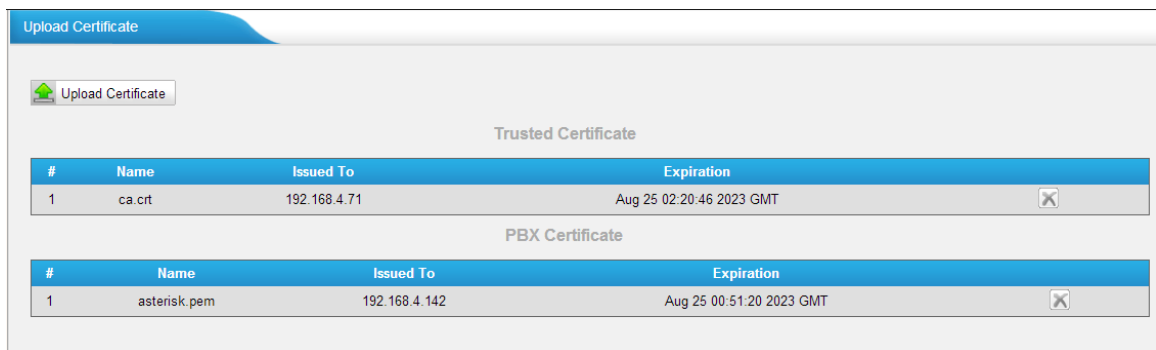


Figure 1-30

The certificates in MyPBX side are uploaded well.

1.4 Register IP phone to MyPBX via TLS

Before register IP phone to MyPBX, we need create a SIP extension in MyPBX side in advance, or edit the exist one. In this example, extension number is 303

We need set TLS protocol in this page, click save and 'apply the changes' on web.

Edit Extension - 303

General | Other Settings

General

Type: SIP | Extension: 303 | Password: pincode303
Name: 303 | Caller ID: 303

Voicemail

Enable Voicemail | Voicemail Access PIN #: 303

Mail Setting

Enable Send Voicemail
Email Address:

Note: Please ensure that the section 'SMTP Settings for Voicemail'(in the 'Voicemail Settings') have been properly configured before using this feature.

Group

Pickup Group: ---

Call Duration Setting

Max Call Duration: s

VoIP Settings

NAT: | Qualify: | Enable SRTP:
Transport: TLS | DTMF Mode: RFC2833 | Register Remotely:

Save | Cancel

Figure 1-31

Open IP phone's configuration page, input the registry information of extension 303

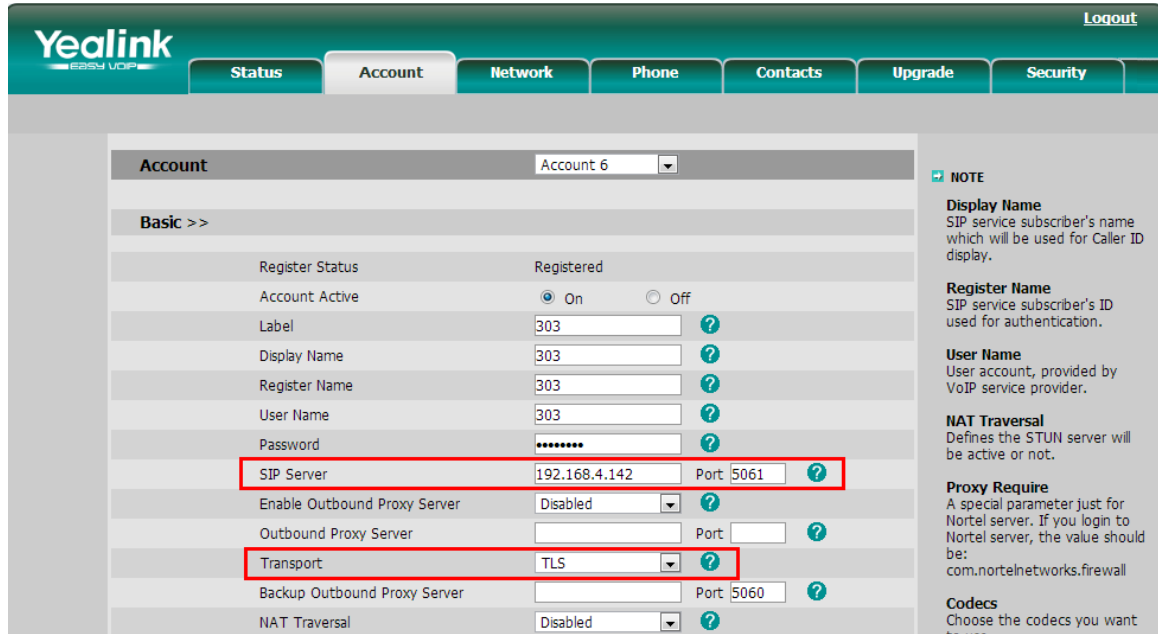


Figure 1-32

Click 'confirm' to apply the changes, then extension 303 is registered well via TLS.

We can also check the status in 'extension status' page of MyPBX.

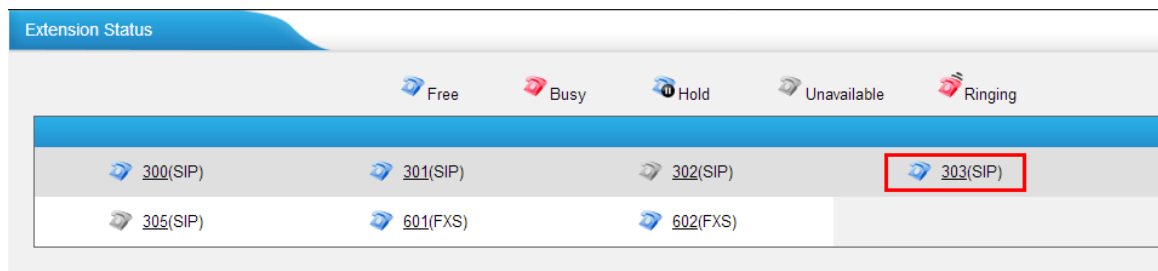


Figure 1-33

If you have any problems about extension's registry, please do a trace in 'Reports→system logs→Capture tool', input ip phone's IP address, choose the eth port, then click 'start', MyPBX will start to do a trace, you can register the IP phone again, then click 'stop' and download the package to analyze via wireshark. You can also send it to analyze.

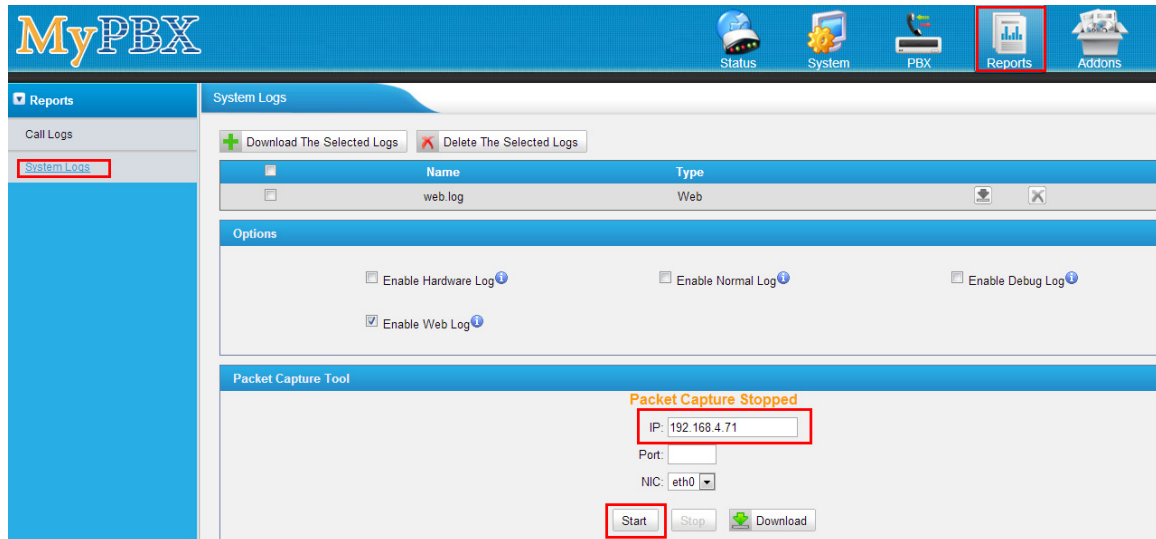


Figure 1-34

2. How to register SIP trunk to VoIP provider via TLS

If you have got the SIP trunk from provider that is using TLS, we can configure it in MyPBX and choose TLS within the trunk, here are two examples for you.

VoIP trunk:

Add VoIP trunk X

Type: SIP

Provider Name: Yeastar

Hostname/IP: 110.80.36.111 : 5060

Domain: 110.80.36.111

User Name: harry

Authorization Name: harry

Password:

From User:

Online Number:

Maximum Channels: 0

Caller ID: 1353478

Realm: yeastar

Enable Outbound Proxy Server

Transport: TLS Enable SRTP: Qualify:

DTMF Mode: rfc2833

Diversion:

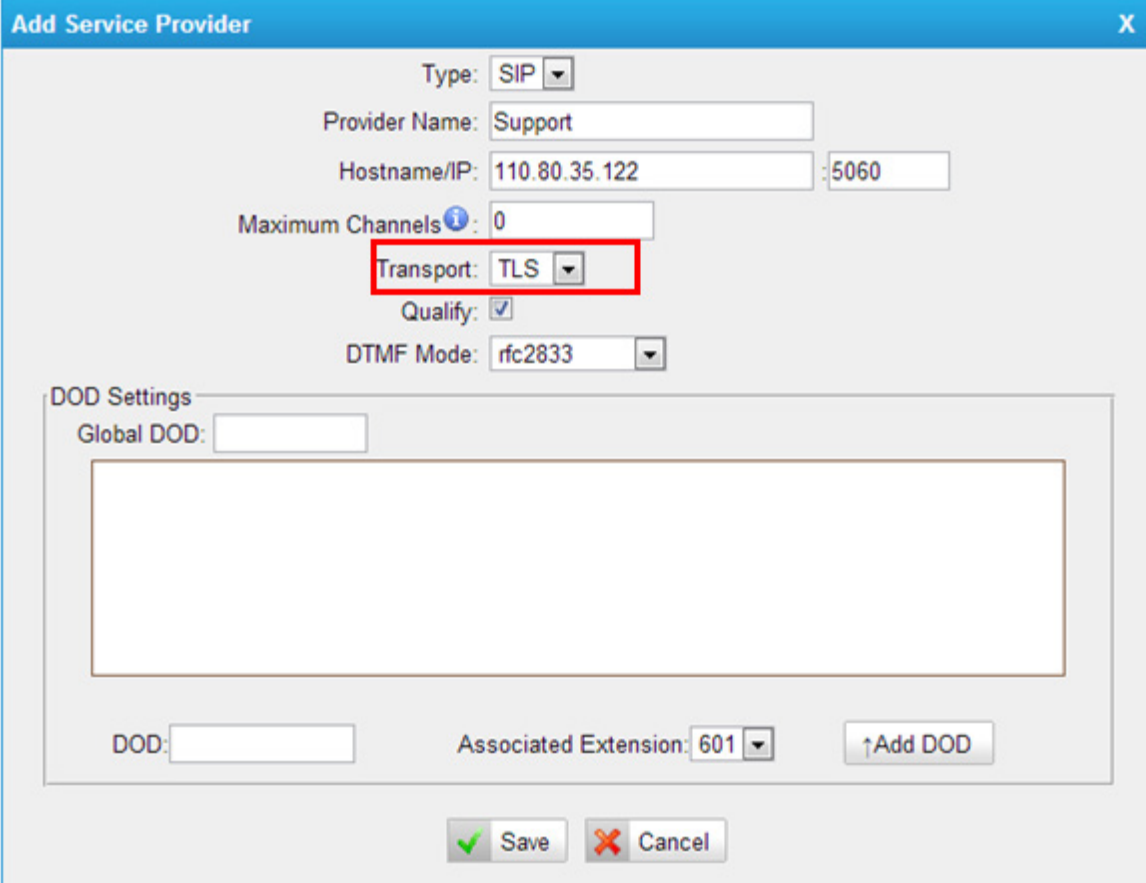
DOD Settings

DOD: Associated Extension: 601 Add DOD

Save Cancel

Figure 2-1

Service provider trunk (P-P).



The screenshot shows the 'Add Service Provider' dialog box with the following fields and values:

- Type: SIP
- Provider Name: Support
- Hostname/IP: 110.80.35.122 : 5060
- Maximum Channels: 0
- Transport: TLS (highlighted with a red box)
- Qualify:
- DTMF Mode: rfc2833

The 'DOD Settings' section includes:

- Global DOD: [empty text box]
- DOD: [empty text box]
- Associated Extension: 601
- ↑Add DOD button

At the bottom are 'Save' and 'Cancel' buttons.

Figure 2-2

If you have got problem when registering to provider via TLS, you can also do a trace in 'system log' page using 'Capture tool', then send it to provider or us to analyze.

[Finish]

