

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	
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	



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



MyPBX		Status	System	PBX
Extensions	SIP Settings			
D Trunks	General NAT Codecs QOS Advanced Settings			
Dutbound Call Control	UDP Port	5060]	
Inbound Call Control	Enable TCP Port	5060]	
Audio Settings	Enable TLS Port 0:	5061		
Basic Settings	TLS Verify Server♥: TLS Verify Client♥:	No •		
Advanced Settings	TLS Ignore Common Name 0:	Yes		
SIP Settings	TLS Client Method :	sslv2 -		
IAX Settings	RTP Port Start.	12000	J	
Blacklist	DTMF Mode Max Registration/Subscription Time	rfc2833 💌 3600]	

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.



MyPBX	, Status System PBX
Extensions	SIP Settings
Trunks	General NAT Codecs QOS Advanced Settings
Outbound Call Control	UDP Port: 5060
Inbound Call Control	Enable TCP Port : 5060
Audio Settings	
Basic Settings	TLS Verify Serverີ♥: No ▼ TLS Verify Client ♥: Yes ▼
Advanced Settings	TLS Ignore Common Name : No
SIP Settings	TLS Client Method 1: sslv2
IAV Sottings	RTP Port Start: 10000
Blacklist	DTMF Mode : ffc2833



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:



				1		x
	CA_T	[ool	▼ 4 ₂	Search TLS_CA_Tool	_	٩
<u>File E</u> dit <u>V</u> iew <u>T</u> o	ols	<u>H</u> elp				
Organize 👻 Inclue	de in	library Share with Burn	New folder	8	≣ ▼ 🗍	?
☆ Favorites	-	Name	Date modified	Туре	Size	
📃 Desktop		🚳 ca	2013/8/7 10:17	Windows Batch File	2 KB	
🐌 Downloads		🚳 client	2013/8/6 20:16	Windows Batch File	1 KB	
💝 Dropbox		🚳 libeay32.dll	2013/4/23 11:29	Application extens	1,398 KB	
🖳 Recent Places		🚳 libssl32.dll	2013/4/23 11:29	Application extens	478 KB	
		🖻 openssl	2013/8/7 9:55	CONF File	4 KB	
🥽 Libraries	Ξ	💷 openssl	2013/4/23 11:29	Application	1,645 KB	
Documents		🚳 server	2013/8/7 10:49	Windows Batch File	1 KB	
🁌 Music						
Pictures						
Subversion						
Videos						
📄 迅雷下载						
🤣 Homegroup						
🖳 Computer						
🚢 Local Disk (C:)	-					
7 items						

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
. + + + + + + +
                                                                                     Ξ
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 NameØ (eg, ip address, website) []:192.168.4.142
Common Namel (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



~~~					x
	Tool 🕨	<b>▼</b> 4 <del>j</del>	Search TLS_CA_Tool	_	P
File Edit View Tools	Help				
Organize 🔻 🗦 Open	Include in library 👻 Share with 👻	Burn New folder		≣ ▼ 🔳	0
🔶 Favorites	Name	Date modified	Туре	Size	
🧮 Desktop	🔰 ca	2013/8/27 8:44	File folder		
📕 Downloads	🚳 ca	2013/8/7 10:17	Windows Batch File	2 KB	
💝 Dropbox	🔄 ca	2013/8/27 8:45	Security Certificate	1 KB	
🔚 Recent Places	🚳 client	2013/8/6 20:16	Windows Batch File	1 KB	
	🚳 libeay32.dll	2013/4/23 11:29	Application extens	1,398 KB	
🥃 Libraries 🛛 🗉	🚳 libssl32.dll	2013/4/23 11:29	Application extens	478 KB	
Documents	🖉 openssl	2013/8/7 9:55	CONF File	4 KB	
J Music	💷 openssl	2013/4/23 11:29	Application	1,645 KB	
Pictures	🚳 server	2013/8/7 10:49	Windows Batch File	1 KB	
Subversion					
🛃 Videos					
📄 迅雷下载					
🍓 Homegroup					
🖳 Computer					
🚢 Local Disk (C:) 🔻					
ca Date File folder	modified: 2013/8/27 8:44				

Figure 1-6

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

								-
COV TLS_C	A_Tool ⊧ ca ⊧	trusted		<b>→</b> 4	Search trusted			Q
File Edit View Too	ls Help							
Organize 👻 Includ	e in library 🔻	Share with 🔻	Burn	New folder				?
☆ Favorites	^ Name	^		Date modified	Туре	Size		
🧮 Desktop	🗔 ca			2013/8/27 8:45	Security Certificate		1 KB	
🗼 Downloads	Ca.csr			2013/8/27 8:45	CSR File		1 KB	
💝 Dropbox	🔄 ca			2013/8/27 8:45	Security Certificate		1 KB	
📃 Recent Places	a.key			2013/8/27 8:44	KEY File		1 KB	
<ul> <li>□ Libraries</li> <li>□ Documents</li> <li>□ Music</li> <li>□ Pictures</li> <li>□ Subversion</li> <li>□ Videos</li> <li>□ 迅雷下载</li> </ul>	E							
vi Homegroup 1. Computer								
🚢 Local Disk (C:)	-							
4 items								

Figure 1-7



 $\sim$ 

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'.

	1000	ALC: NO. OF TAXABLE PARTY.	1.00		x
	Tool 🕨	<b>▼</b> 4 ₇	Search TLS_CA_Tool		Q
File Edit View Tools	Help				
Organize 🔻 📑 Open	Share with 🔻 Print Burn	New folder		≣ ▼ 🗍	?
☆ Favorites	Name	Date modified	Туре	Size	
Nesktop	鷆 ca	2013/8/27 8:44	File folder		
〕 Downloads	🚳 ca	2013/8/7 10:17	Windows Batch File	2 KB	
💔 Dropbox	🔄 ca	2013/8/27 8:45	Security Certificate	1 KB	
📃 Recent Places	🚳 client	2013/8/6 20:16	Windows Batch File	1 KB	
	🚳 libeay32.dll	2013/4/23 11:29	Application extens	1,398 KB	
🥃 Libraries 🗧	🚳 libssl32.dll	2013/4/23 11:29	Application extens	478 KB	
Documents	🗹 openssl	2013/8/7 9:55	CONF File	4 KB	
🁌 Music	💷 openssl	2013/4/23 11:29	Application	1,645 KB	
Pictures	🐼 server	2013/8/7 10:49	Windows Batch File	1 KB	
Subversion					
😸 Videos					
🔒 迅雷下载 📃					
🝓 Homegroup					
🖳 Computer					
🚢 Local Disk (C:) 🔻					
Server Windows Batch	Date modified: 2013/8/7 10:49 File Size: 898 bytes	Date created: 2013/8/26 2	2:31		

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.





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.



	CONTRACTOR OF TAXABLE		Contraction of the local division of the loc		x
	Tool 🕨	<b>▼</b> 49	Search TLS_CA_Tool		٩
File Edit View Tools	Help				
Organize 👻 📄 Open	Share with 🔻 🛛 Burn 🛛 New folder			•	?
★ Favorites	Name	Date modified	Туре	Size	
Nesktop	퉬 ca	2013/8/27 8:52	File folder		
🗼 Downloads	rnd	2013/8/27 8:52	RND File	1 KB	
💝 Dropbox	asterisk.pem	2013/8/27 8:52	PEM File	2 KB	
🔚 Recent Places	🚳 ca	2013/8/7 10:17	Windows Batch File	2 KB	
	🙀 ca	2013/8/27 8:45	Security Certificate	1 KB	
🥃 Libraries 🛛 🗉	🚳 client	2013/8/6 20:16	Windows Batch File	1 KB	
Documents	🚳 libeay32.dll	2013/4/23 11:29	Application extens	1,398 KB	
J Music	🚳 libssl32.dll	2013/4/23 11:29	Application extens	478 KB	
Pictures	🖉 openssl	2013/8/7 9:55	CONF File	4 KB	
Subversion	💷 openssl	2013/4/23 11:29	Application	1,645 KB	
🛃 Videos	Server	2013/8/7 10:49	Windows Batch File	1 KB	
📄 迅雷下载					
🖏 Homegroup					
Local Disk (C:)					
asterisk.pem I PEM File	Date modified: 2013/8/27 8:52 Date crea Size: 1.94 KB	ted: 2013/8/27 8:52			

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.



10.00								x
🕞 🕞 🗸 🕨 Certi	ificate 🕨 MyPBX_0	ertificate		<b>▼ ⁴?</b>	Search MyPBX_certific	ate		٩
File Edit View To	ols Help							
Organize 🔻 Inclu	ide in library 🔻	Share with 🔻 🛛 🛛 B	urn New fo	lder		-		0
☆ Favorites	^ Name	^		Date modified	Туре	Size		
Desktop Downloads Dropbox Recent Places	🗋 asterisl	.pem		2013/8/27 8:52 2013/8/27 8:45	PEM File Security Certificate		2 KB 1 KB	
<ul> <li>⇒ Libraries</li> <li>È Documents</li> <li>J Music</li> <li>⇒ Pictures</li> <li>⇒ Subversion</li> <li>₩ Videos</li> <li>⇒ 迅雷下载</li> </ul>	H							
v Homegroup III Computer Local Disk (C:)	-							
2 items								

Figure 1-11 Step3. Prepare the IP phone's certificate, ca.crt

							x
	CA_T	[ool		<b>▼</b> 4 ₂	Search TLS_CA_Tool		٩
File Edit View To	ols	Help					
Organize 👻 Inclu	de in	library 👻 Share with 👻	Burn	New folder	1	•	0
▲ ★ Favorites		Name		Date modified	Туре	Size	
🧮 Desktop		🚳 ca		2013/8/7 10:17	Windows Batch File	2 KB	
\rm 😺 Downloads		🚳 client		2013/8/6 20:16	Windows Batch File	1 KB	
😻 Dropbox		🚳 libeay32.dll		2013/4/23 11:29	Application extens	1,398 KB	
📃 Recent Places		🚳 libssl32.dll		2013/4/23 11:29	Application extens	478 KB	
		📓 openssl		2013/8/7 9:55	CONF File	4 KB	
4 演 Libraries	Ξ	💷 openssl		2013/4/23 11:29	Application	1,645 KB	
Documents		🚳 server		2013/8/7 10:49	Windows Batch File	1 KB	
🖻 🎝 Music							
Pictures							
Subversion							
Videos							
▷ 📄 迅雷下载							
🖻 輚 Homegroup							
4 🖳 Computer							
b 💒 Local Disk (C:)	-						
7 items							

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.

_ D X C:\Windows\system32\cmd.exe Loading 'screen' into random state – done ٠ Generating RSA private key, 1024 bit long modulus III ***** . + + + + + + 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 NameØ (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.



					and the second second		x
	CA_T	Tool 🕨		<b>▼</b> 49	Search TLS_CA_Tool		٩
File Edit View To	ols	Help					
Organize 🔻 Inclu	de in	library 🔻 Share with 👻 Burn	New fo	older		≡ ▼ 🗍	0
☆ Favorites	-	Name		Date modified	Туре	Size	
🧮 Desktop		鷆 ca		2013/8/27 10:10	File folder		
🗼 Downloads		🚳 ca		2013/8/7 10:17	Windows Batch File	2 KB	
💝 Dropbox		🛱 ca		2013/8/27 10:20	Security Certificate	1 KB	
📃 Recent Places		🚳 client		2013/8/6 20:16	Windows Batch File	1 KB	
		🚳 libeay32.dll		2013/4/23 11:29	Application extens	1,398 KB	
演 Libraries	Ξ	🚳 libssl32.dll		2013/4/23 11:29	Application extens	478 KB	
Documents		🖻 openssl		2013/8/7 9:55	CONF File	4 KB	
👌 Music		💷 openssl		2013/4/23 11:29	Application	1,645 KB	
Pictures		🚳 server		2013/8/7 10:49	Windows Batch File	1 KB	
Subversion							
📑 Videos							
📄 迅雷下载							
輚 Homegroup							
🖳 Computer							
🚢 Local Disk (C:)	Ŧ						
9 items							

Figure 1-14

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

								x
	CA_Tool ト ca ト	trusted		<b>▼</b> 47	Search trusted			P
File Edit View To	ols Help					_	_	-
Organize 🔻 🛛 Inclu	de in library 🔻	Share with 🔻	Burn	New folder		-		?
☆ Favorites	▲ Name	*		Date modified	Туре	Size		
Nesktop	🗔 ca			2013/8/27 10:20	Security Certificate		1 KB	
鷆 Downloads	ca.csr			2013/8/27 10:10	CSR File		1 KB	
💔 Dropbox	🔄 ca			2013/8/27 10:20	Security Certificate		1 KB	
📃 Recent Places	a.key			2013/8/27 10:10	KEY File		1 KB	
<ul> <li>□ Libraries</li> <li>□ Documents</li> <li>→ Music</li> <li>□ Pictures</li> <li>□ Subversion</li> <li>□ Videos</li> <li>□ 迅雷下载</li> </ul>	Ш							
🔣 Homegroup								
Computer	-							
4 items								

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'.** 

	_Tool →	✓ 4→ Search	TLS_CA_Tool
File Edit View Tools	Help		
Organize 🔻 🖬 Oper	n Share with 🔻 Print Burn	New folder	:= - 🔟 🔞
☆ Favorites	Name	Date modified Type	e Size
Desktop	\mu ca	2013/8/27 10:10 File f	older
🚺 Downloads	🚳 ca	2013/8/7 10:17 Wind	dows Batch File 2 KB
💔 Dropbox	ca	2013/8/27 10:20 Secu	rity Certificate 1 KB
🖳 Recent Places	🔊 client	2013/8/6 20:16 Wind	dows Batch File 1 KB
	🔊 libeay32.dll	2013/4/23 11:29 Appl	ication extens 1,398 KB
🥽 Libraries 🛛 🗉	🔊 libssl32.dll	2013/4/23 11:29 Appl	ication extens 478 KB
Documents	🖉 openssl	2013/8/7 9:55 CON	IF File 4 KB
J Music	🔲 openssl	2013/4/23 11:29 Appl	ication 1,645 KB
Pictures	Server	2013/8/7 10:49 Wind	dows Batch File 1 KB
Subversion			
😽 Videos			
🔒 迅雷下载			
🍓 Homegroup			
🖳 Computer			
🚢 Local Disk (C:) 🔻			
Client Windows Batch	Date modified: 2013/8/6 20:16 h File Size: 594 bytes	Date created: 2013/8/26 22:31	

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
                                                . . . + + + + + + +
Ε
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 NameØ (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'
common Name
                     :PRINTABLE:'192.168.4.71'
Certificate is to be certified until Aug 25 02:30:44 2023 GMT <3650 days)
sign the certificate: Ly/nl: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.



						x			
C→ → TLS_0	CA_T	iool 🕨	<b>- - i i j −</b>	Search TLS_CA_Tool		Q			
<u>File Edit View I</u> ools <u>H</u> elp									
Organize 🔻 Include in library 👻 Share with 👻 Burn New folder 🛛 📰 💌 🗍 🔞									
Favorites	-	Name	Date modified	Туре	Size				
Desktop		📔 ca	2013/8/27 10:34	File folder					
Downloads		.rnd	2013/8/27 10:34	RND File	1 KB				
💔 Dropbox		 ③ ca	2013/8/7 10:17	Windows Batch File	2 KB				
💷 Recent Places		🔄 ca	2013/8/27 10:20	Security Certificate	1 KB				
		🚳 client	2013/8/6 20:16	Windows Batch File	1 KB				
演 Libraries	Ξ	client.pem	2013/8/27 10:34	PEM File	2 KB				
Documents		🚳 libeay32.dll	2013/4/23 11:29	Application extens	1,398 KB				
🁌 Music		🚳 libssl32.dll	2013/4/23 11:29	Application extens	478 KB				
Pictures		📝 openssl	2013/8/7 9:55	CONF File	4 KB				
Subversion		openssl	2013/4/23 11:29	Application	1,645 KB				
😽 Videos		🚳 server	2013/8/7 10:49	Windows Batch File	1 KB				
📄 迅雷下载									
🤣 Homegroup									
👰 Computer									
🚢 Local Disk (C:)	-								
11 items									

Figure 1-18

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

						x
🕒 🗢 📕 🕨 Certi	ificate 🕨 IP Phone_certificate	<b>-</b> ↓	Search IP Phone_certi	ficate		P
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> o	ols <u>H</u> elp					
Organize 🔻 Inclu	ide in library 👻 Share with 👻 Burn 🛛	New folder	l	-		?
☆ Favorites	▲ Name	Date modified	Туре	Size		
Desktop Downloads Dropbox Recent Places	🛱 ca 🗋 client.pem	2013/8/27 10:20 2013/8/27 10:34	Security Certificate PEM File		1 KB 2 KB	
<ul> <li>➢ Libraries</li> <li>➢ Documents</li> <li>➢ Music</li> <li>➢ Pictures</li> <li>➢ Subversion</li> <li>☑ Videos</li> <li>☑ 迅雷下载</li> </ul>	Ξ					
vi Homegroup I						
2 items						

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

sy vop	Status	Account	Network	Phone	Contacts	Upgrade	Security
		Password	Trusted Certifica	tes   Server Cer	tificates		
	Issued To	Issued By	Expira	ation	Delete	D NOTE	
	Upload Server Certifica	te	Choose File No file	chosen	Upload		

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.



ade Se
NOTE
NOTE
×
tificate 🔎
·
Туре
Security C
PEM File

Figure 1-21

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

Yea	link		_	_		_	_	Loqout
E35-	VOP	Status	Account	Network	Phone	Contacts	Upgrade	Security
			Password	Trusted Certifica	ates Server Cer	tificates		
	Is 192	ssued To 2.168.4.71 In	Issued By Iternet Widgits Pty Ltd	Expir Aug 25 02:30	ation :44 2023 GMT	Delete Delete	D NOTE	
	ι	Jpload Server Certifi	icate [	Choose File) No fil	e chosen	Upload		

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.



Yeo	llink								<u>Logout</u>
Eas	VOP	Status	Account	Network	Phone	$\gamma$	Contacts	Upgrade	Security
			Password	Trusted Cer	tificates Server	Certificat	tes		
	Index 1 2	Issued To Thawte Premium Server CA	Issued By VeriSign, In Thawte Consult	c. Auç ing cc Jan	Expiration 2 23:59:59 2028 GM 1 23:59:59 2021 GM	IT T	Delete	🖬 NOTE	
	3 4 5 6				Open € ↓ Certi	ificate )	MyPBX_certificat	ie 🗸	4→ Search MyPBX_certifi
	7 8 9				Organize ▼ New	folder	Name	*	8़≡≡ ▼ Date modified
	10				💻 Desktop ᠾ Downloads 🍄 Dropbox	=	asterisk.pem		2013/8/27 8:52 2013/8/27 8:45
		Only Accept Truste	d Certificates		Recent Places Libraries				
		Import Trusted Co	ertificate (.crt,.cr	er) ile No file ch	<ul> <li>Documents</li> <li>Music</li> <li>Pictures</li> <li>Subversion</li> </ul>				
			Confirm		📕 Videos F	+ + File name	e: ca	m	✓ All Files

Figure 1-23



Figure 1-24

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



Yea	link						
E355	VOP	Status	Account	Network	Phone	Contacts	Up
			Password	Trusted Certif	icates Server Cer	tificates	
							_
	Index	Issued To	Issued By		Expiration	Delete	
	1		VeriSign, Inc	. Aug 2	23:59:59 2028 GMT		
	2	192.168.4.142	Internet Widgits P	ty Ltd Aug 25	00:45:15 2023 GMT		
	3	hawte Premium Servei CA	^r Thawte Consultir	ng cc Jan 1	23:59:59 2021 GMT		
	4						
	5						
	6						
	7						
	8						
	9						
	10						
						Delete	
		Only Accept Trust	ed Certificates		Enabled 💌	]	

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.

MyPBX	Status System PBX Reports Addons Logout
Extensions	Upload Certificate
Trunks	
Outbound Call Control	Le Upload Certificate
Inbound Call Control	Trusted Certificate
Audio Settings	Upload Certificate X
Basic Settings	Type: PBX Certificate
Advanced Settings	Choose a centricate to Upload Choose File Open
SIP Settings	Save Save Cancel MyPBX_certificate + 49 Search MyPBX_certificate P
IAX Settings	Organize ▼ New folder III ▼ □ 0
Blacklist	Arenice     A
Callback Settings	Downloads = Ca 2013/8/27 8:45 Security C
DNIS Settings	
DISA	Cip Libraries
PIN User Settings	Documents
Paging Groups	Pictures     Subversion
SMS Settings	Videos V ( W
<u>Cerificates</u>	File name: asterisk.pem

Figure 1-26



Upload Cer	rtificate			Apply Changes
全 Uploa	ad Certificate			
		Trus	ted Certificate	
		N	o Certificates Defined	
		PE	3X 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!	

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

Figure 1-27

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

Upload Cert	lificate								
Lupload Certificate									
	Trusted Certificate								
No Certificates Defined									
		PB>	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.



Upload Certificate						
Upload Certificate Upload Certificate Choose a ceritificate	Type: Trusted Certificate  o Upload: Choose File No file c Save Cancel Issued To	Open Organize → New for Favorites ■ Desktop	v iate • IP Phone_certificate Ider Name	▼ 49 Sea	rch IP Phone_certifi ∃∷ ▼ Date modified 2013/8/27 10:20	icate P Type Security C
1 asterisk.pem	192.168.4.142	<ul> <li>Downloads</li> <li>Propbox</li> <li>Recent Places</li> <li>Libraries</li> <li>Documents</li> <li>Music</li> <li>Pictures</li> <li>Subversion</li> <li>Videos</li> </ul>	cient.pem	™ - All Fi	2013/8/27 10:34	PEM File

Figure 1-29

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

opioad Centricate	
🚖 Upload Certificate	
Trusted Certificate	
# Name Issued To Expiration	
1 ca.crt 192.168.4.71 Aug 25 02:20:46 2023 GMT	×
PBX Certificate	
# Name Issued To Expiration	
1 asterisk.pem 192.168.4.142 Aug 25 00:51:20 2023 GMT	×

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.



dit Extension - 303	х
General Other Settings	
[ General	
Type: SIP - Extension 1: 303 Password 2: 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')	
nave been property conligured before using this reactive.	
Group	
Pickup Group	
Call Duration Setting	
Max Call Duration 0: s	
VoIP Settings	
NAT 🛈 : 🗖 Qualify: 🗹 Enable SRTP 🛈 : 🗖	
Transport: TLS 🔽 DTMF Mode 🛈 : RFC2833 💌 Register Remotely 🛈 : 🗉	
Save Save	1

Figure 1-31

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



Veglink	-						<u>Loqout</u>
	Status	Account	Network	Phone	Contacts	Upgrade	Security
Account			Account	6 💌			
						NOTE	
Basic >>						Displa SIP se which	y Name rvice subscriber's name will be used for Caller ID
	Register S	itatus	Registered	ł		display	•
	Account A	Active	On	O Off		Regis	ter Name
	Label		303			used f	or authentication.
	Display Na	me	303	0		User I	lame
	Register N	lame	303	()		User a VoIP s	ccount, provided by ervice provider.
	User Nam	e	303	0		Τ ΤΑΛ	raversal
	Password		•••••	0		Define be act	s the STUN server will
	SIP Serve	r	192.168.4	142 Por	t 5061 🕜	Deaco	Beering.
	Enable Ou	itbound Proxy Server	Disabled	- (		A spe	tial parameter just for
	Outbound	Proxy Server		Por	t 📃 🕜	Nortel	server. If you login to server, the value should
	Transport		TLS	- (		be: com.n	ortelnetworks.firewall
	Backup O	utbound Proxy Server		Por	t 5060 🕜	Code	
	NAT Trav	ersal	Disabled	- (	)	Choos	e the codecs you want

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.

Ð	tension Status					
		Free	🔊 _{Busy}	a Hold	🔊 Unavailable	arr Ringing
	300(SIP)	301(SIP)		302(SIP)		303(SIP)
	305(SIP)	<u>601(FXS)</u>		<u>602(FXS)</u>		
L						

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.



MyPBX			Status System	PBX Reports Addons
Reports	System Logs			
Call Logs	+ Download The Se	elected Logs 📉 Delete The Selected Logs		
System Logs		Name	Туре	
		web.log	Web	
	Options			
		Enable Hardware Log	Enable Normal Log ¹	Enable Debug Log ¹
		Enable Web Log		
	Packet Capture To	pol		
			Packet Capture Stopped	
			Start Stop 👱 Download	



# 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 ⁽¹⁾ :	yeastar
	Enable Outbound Proxy Server
Transport:	TLS  Enable SRTP
DTMF Mode:	rfc2833
Diversion :	
DOD Settings	
DOD:	Associated Extension: 601  Add DOD
	Save X Cancel

Figure 2-1

Service provider trunk (P-P).



Service Provider		
Туре:	SIP 💌	
Provider Name:	Support	]
Hostname/IP:	110.80.35.122	: 5060
Maximum Channels 🛈 :	0	
Transport:	TLS 💌	
Qualify:		
DTMF Mode:	rfc2833	
Global DOD:		
DOD: As	sociated Extension: 601 💌	↑Add DOD
<b>~</b>	Save 🔀 Cancel	

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]



