راه اندازی TLS/SRTP در تلفنهای Akuvox و مرکز تلفن Yeastar

یکی از قابلیتهایی که تلفنهای تحت شبکه آکووکس پشتیبانی میکنند قابلیت استفاده از TLS به جای UDP برای سیگنالینگ و همچنین SRTP برای امنیت انتقال صدا میباشد. در این آموزش ما از یک تلفن مدل Akuvox R59P به عنوان کلاینت و از مرکز تلفن یستار Yeastar استفاده خواهیم کرد.

عربین مرزمین شروعی عمل میں معلم معلم معرف معلم به عنون عریف ورمر مرغ عمل یستار معاملات مستقل علم عرف عرف **«نکته بسیار مهم:** لازم به ذکر است در صورت صحیح نبودن تنظیمات تاریخ و ساعت بر روی تلفن، ارتباط TLS در نهایت برقرار نخواهد شد. بنابراین بهتر است قبل از شروع تنظیمات، تاریخ و ساعت تلفن را بررسی و در صورت اشتباه بودن آن را اصلاح کنید.

تنظيمات:

گام اول: ساخت Certificate

در ابتدا لازم است تا یک certificate برای مرکز تلفن یستار ایجاد نمایید. برای این کار ابتدا فایل <u>TLS CA Tool</u> را دانلود کرده و از حالت فشرده خارج کنید.

🕖 🖉 📕 🕨 TLS	_CA_Tool				+ + Search	TLS_CA_Tool	100	
Organize 👻 Incl	ude in library 🔻	Share with 🔻	Burn	New folder		F	8≣ ▼	0
😭 Favorites	Name	<u>^</u>		Date modified	Туре	Size		
Desktop	🚳 ca.bat			2013/8/7 10:17	Windows Batch File	2 KB		
😹 Downloads	🚳 client.bat			2013/8/6 20:16	Windows Batch File	1 KB		
🔠 Recent Places	🚳 libeay32.dll			2013/4/23 11:29	Application extens	1,398 KB		
	libssl32.dll			2013/4/23 11:29	Application extens	478 KB		
词 Libraries	openssl.conf			2013/8/7 9:55	CONF File	4 KB		
Documents	🗾 openssl.exe			2013/4/23 11:29	Application	1,645 KB		
J Music	server.bat			2013/8/7 10:49	Windows Batch File	1 KB		

در مرحلهی اول روی ca.bat کلیک کرده و در صفحه اول ابتدا یک رمز دلخواه برای ca key وارد نمایید.





نکته: برای پارامتر common name آدرس آیپی سرور Yeastar را وارد کنید.



در حال حاضر در پوشه فعلی یک فایل Ca و یک فولدر Ca ساخته شده است، لازم به ذکر است فایل Ca که داخل پوشه Ca قرار دارد با

					×
	iool >	▼ 4 9	Search TLS_CA_Tool		٩
File Edit View Tools	Help				
Organize 🔻 🛛 🏹 Open	Include in library	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	Ep 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	😰 openssi	2013/8/7 9:55	CONF File	4 KB	
J Music	📧 openssi	2013/4/23 11:29	Application	1,645 KB	
E Pictures	server	2013/8/7 10:49	Windows Batch File	1 KB	
Subversion					
🚼 Videos					
過 迅雷下载					
🔞 Homegroup					
Computer					
Ca Date File folder	modified: 2013/8/27 8:44				

فایل Ca در همین پوشه یکی میباشد.



در مرحله دوم روی فایل server.bat کلیک کرده و اطلاعات را دقیقا مانند ca.bat که در مرحله قبل وارد شد وارد نمایید. در نهایت برای سوال اول و دوم "y" وارد کرده و Enter کنید. - 0 X C:\Windows\system32\cmd.exe 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]:FJ Locality Name (eg, city) []:XM Prganization Name (eg, company) [Internet Widgits Pty Ltd]:Yeastar Organizational Unit Name (eg, section) []: Common NameØ (eg, ip address, website) []:192.168.6.216 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 []:ys123456 An optional company name Ll: Using configuration from openssl.conf Loading 'screen' into random state – done Enter pass phrase for ca\trusted\ca.key: 15140:error:28069065:lib(40):UI_set_result:result too small:./crypto/ui/ui_lib.c :847:You must type in 4 to 511 characters 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 :PRINTABLE:'CN' countryName :PRINTABLE:'FJ' stateOrProvinceName :PRINTABLE:'XM' localityName :PRINTABLE:'Yeastar' organizationName :PRINTABLE:'192.168.6.216' commonName Certificate is to be certified until Mar 1 11:41:22 2027 GMT (3650 days) Sign the certificate? [y/n]:y out of 1 certificate requests certified, commit? [y/n]y در نهایت فایل asterisk.pem داخل فولدر فعلی ساخته خواهد شد

حال برای مرحله سوم روی client.bat کلیک کرده و مجدد مانند مراحل قبل اطلاعات را وارد کنید.



C:\Windows\system32\cmd.exe		x
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]:FJ Locality Name (eg, city) []:XM Organization Name (eg, company) [Internet Widgits Pty Ltd]:Yeastar Organizational Unit Name (eg, section) []: Common NameØ (eg, ip address, website) []:192.168.6.113 Common Name1 (eg, ip address, website) []: Common Name1 (eg, ip address, website) []: Email Address []:		н
Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []; ys123456 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:'FJ' localityName :PRINTABLE:'XM' organizationName :PRINTABLE:'Yeastar' commonName :PRINTABLE:'192.168.6.113' Certificate is to be certified until Mar 1 12:07:48 2027 GMT (3650 d Sign the certificate? [y/n]:y	ays)	
1 out of 1 certificate requests certified, commit? [y/n ly		

در نهایت فایل client.pem داخل فولدر فعلی ایجاد خواهد شد .

در حال حاضر شما سه فایل ca.crt و asterisk.pem و client.pem را در اختیار دارید.

گام دوم: بارگذاری certificate در مرکز تلفن

در مرحلهی بعد وارد محیط گرافیکی Yeastar شده و مسیر زیر را طی کنید:

Settings >Security >Certificates

در این صفحه روی Upload کلیک کرده و ابتدا Type را روی PBX Certificate گذاشته و فایل asterisk.pem را آپلود نمایید. سپس مجدد روی Upload کلیک کرده و Type را روی Trusted Certificate قرار داده و این بار فایل Ca.crt را هم آپلود کنید. در نهایت مانند تصویر زیر ۲ عدد فایل آپلود شده خواهیم داشت:

Settings							$-\Box \times$
> PBX	Firewa	ll Rules	IP Auto Defense	Service	Certificate	Database Grant	
 System Network 	Upload	Delete					
Security		Name	Ту	ре	Issue To	Expiration	Delete
User Permission		asterisk.pem	PBX Ce	ertificate	192.168.1.14	1 May 10 10:28:40 2028	İ
Date & Time		ca.crt	Trusted (Certificate	192.168.1.14	1 May 10 10:28:09 2028	面
Email							
Storage							
Remote Management							
Hot Standby							
Event Center							



گام سوم: تنظیمات TLS در مرکز تلفن

د زیر انجام دهید:	نظيمات را مانند	ده و ت	Settin ش	gs >Gen	eral >S	SIP >TI	مسیر S۔	گاه وارد ه	، مجدد دستًا	َن راہاندازی
Settings										$-\Box \times$
V PBX	Preferences	Feat	ure Code	Voicemail	SIP	IAX				
Extensions	< General	NAT	Codec	TLS	Session	Timer	QoS	T.38	Advanced	Jitter Bu
Trunks	Enable TLS	1								
Multisite Interconnect		1								
Call Control	TLS Port (1):		5061							
Call Features	Certificate:		asterisk.pe	em 🔻	Certifica	te Settings				
Voice Prompts	TLS Verify Sen	er 🕕								
General										
Recording	TLS Verify Clie	nt 🛈			_					
Emergency Number	TLS Client Method	0:	tlsv1	•						
> System										
> Event Center										

سپس تنظیمات را ذخیره نمایید.

گام چهارم: تنظیمات TLS برای داخلی مورد نظر

برای انجام تنظیمات روی یک Extension وارد مسیر Settings >Extensions شده و برای مثال Extension 1009 را Edit کرای کنید. سپس وارد لبه Advanced شده و نوع Transport را به TLS تغییر دهید.

BX			Edit Exte	ension(1009)			×
Ex	Basic Features	Advanced	Call Permissio	on			
Tri	VoIP Settings						
Mu	S NAT 🛈			🕑 Qualify 🛈			e
Ca	Segister Remotely			🗹 Enable SRTP 🛈			_
Vo	Transport ①:	TLS	-	DTMF Mode ①:	RFC4733	•	
Ge Re En	Enable User Agent	Registration Aut	thorization				
/ste	User Agent:			+			
/er	IP Restriction						
	Enable IP Restriction	Ū					
	Permitted IP/Subnet mas	sk:		1	+		
			20	Cancel			

سپس تنظیمات را ذخیره کنید.

توجه: گزینه register remotely برای کاربران بیرون از شبکه داخلی میبایست فعال گردد.

توجه: با گزینه Enable SRTP، مدیا نیز رمزگذاری می شود.

گام پنجم: تنظیمات داخلی در تلفن Akuvox

پس از تعریف داخلی مورد نظر، وارد محیط گرافیکی پنل تلفن Akuvox شوید. از منوی سمت چپ روی Accounts و سپس زیر منوی Basic، کلیک نمایید.

داخلی مورد نظر که پیشتر در یستار ایجاد شد را را در اینجا تعریف کنید:



Akuvox

Account-Basic		Help
	SIP Account	Note :
Status	Registered	Max length of characters for input
Account	Account 1	box:
Account Active	Enabled 🔻	255: Broadsoft Phonebook server
Display Label	1010	127: Remote Phonehook LIRL &
Display Name	1010	AUTOP Manual Update Server UR
Register Name	1010	63: The rest of input boxes
User Name	1010	
Password	•••••	Warning :
		Field Description :
	SIP Server 1	
Server IP	192,168,1.63 Port 5061	Submit Shortcut
Registration Period	1800 (30~65535s)	Submit Cancel
	SIP Server 2	
Server IP	Port 5060	
Registration Period	1800 (30~65535s)	
-		
Out	bound Proxy Server	
Enable Outbound	Disabled V	
Server IP	Port 5060	
Backup Server IP	Port 5060	
	Transport Type	
Transport Type	TLS	
	NAT	
NAT		
INPLI I	Uisabled Y	
Chun Conver Address		

همان طور که دیده میشود، TLS برای Transport Type و پورت TLS برابر با ۵۰۶۱ برای SIP Server 1 که همان آدرس سرور Yeastar میباشد، قرار داده شده است. در نهایت تنظیمات را ذخیره کنید. که در این مرحله داخلی شما رجیستر خواهد شد. همچنین برای فعالسازی SRTP داخل تلفن به مسیر Account >Advanced رفته و داخل صفحه گزینه Encryption را روی Compulsory ست کنید:

	Warning :	
AOC	Disabled v	Field Description :
I	Encryption	Submit Shortcut
Voice Encryption(SRTP)	Compulsory •	Submit Cancel
	NAT	
UDP Keep Alive Messages	Enabled 🔹	
	30 (5~60s)	
UDP Alive Msg Interval	/	

طرفین فعال و در سمت دیگر غیر فعال باشد، تماس برقرار "نخواهد" شد.