?? Asterisk ????? SIP ?? - TLS(Transport Layer Security)?

?????

- PIAF 1.7.5.5 (Asterisk 1.6.2.17)
- CentOS 5.5

?? CA(Certificate Authority)

#mkdir /etc/asterisk/cert #cd /etc/asterisk/cert #openssl genrsa -des3 -out ca.key 4096 Generating RSA private key, 4096 bit long modulus ++ e is 65537 (0x10001) Enter pass phrase for ca.key: ???? Verifying - Enter pass phrase for ca.key: ???? ???(self-signed)?? #openssl reg -new -x509 -days 365 -key ca.key -out ca.crt Enter pass phrase for ca.key: ?? 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) [GB]:TW State or Province Name (full name) [Berkshire]:OSSLab Locality Name (eg, city) [Newbury]:HC Organization Name (eg, company) [My Company Ltd]:OSSLAB

Organizational Unit Name (eg, section) []:OSSLAB

Common Name (eg, your name or your server's hostname) []:<???IP???> Email Address []:

Tips:

? ?? ca.crt ????????? "??????"

???? cacrt ?????? Windows XP) ??? > ?????? > ?? > ?? > ??

- 1. ?? ca.crt ?????
- 3. ????

預定目的心: <全部> 個人 其他人 中繼憑證授權 信任的根憑證授權 受信任的發行者 不受信任此 整給 發行者 到期日 好記的名稱 211.72 211.72 2012/7/15 <無> 公本BA ECOM Root CA ABA ECOM Root CA 2009/7/10 DST (ABA ECO 公本因者 Trust External C Add Trust External CA 2020/5/30 USER Trust 公本 Add Trust External CA 2020/5/30 USER Trust 公本 Add Trust External CA 2009/6/29 Autoridad Certificad Autoridad Certificad Autoridad Certificador 2009/6/29 Autoridad Certifi 公本 Autoridad Certificad Autoridad Certificador 2009/6/30 Autoridad Certifi 公 Autoridad Certificad Autoridad Certificador 2009/7/4 DST (Baltimore Cyber >> Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E >> Belgacom E-Trust P Belgacom E-Trust * >> >> >>	證			?
個人 其他人 中繼憑證授權 信任的根憑證授權 受信任的發行者 不受信任的 凝給 發行者 到期日 好記的名稱 211.72 211.72. 2012/7/15 <無> 四 ABA ECOM Root CA ABA ECOM Root CA ABA ECOM Root CA 2009/7/10 DST (ABA ECO 四 Add Trust External C Add Trust External CA 2020/5/30 USER Trust 四 America Online Roo America Online Root 2037/11/20 America Online R 四 Autoridad Certificad Autoridad Certificador 2009/6/29 Autoridad Certifi 四 Autoridad Certificad Autoridad Certificador 2009/6/30 Autoridad Certifi 四 Baltimore CyberTru Baltimore CyberTrut 2025/5/13 Baltimore Cyber 四 Belgacom E-Trust P Belgacom E-Trust P Belgacom E-Trust ✓ 匯 入① 隆出② 移除 ① 進階(△ 遊 微使用目的 後 (1) (2)	頁定目的(N): <全部	ß>		~
發給 發行者 到期日 好記的名稱 ② 211.72 211.72 2012/7/15 <無> ③ ABA.ECOM Root CA ABA.ECOM Root CA 2009/7/10 DST (ABA.ECO ④ Add Trust External C Add Trust External CA 2020/5/30 USER Trust ④ America Online Roo America Online Root 2037/11/20 America Online R ④ Autoridad Certificad Autoridad Certificador 2009/6/29 Autoridad Certifi ④ Autoridad Certificad Autoridad Certificador 2009/6/30 Autoridad Certifi ⑤ Baltimore CyberTru Baltimore CyberTrust 2025/5/13 Baltimore Cyber ⑤ Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E ⑤ Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trus ▼	個人其他人中繼憑語	證授權 信任的根憑證授	權 受信任的	」發行者 不受信任的 < ▶
Stra Stra Strady-A # 211.72 211.72 211.72 211.72 211.72 211.72 211.72 211.72 211.72 211.72 2012/7/15 ABA ECOM Root CA ABA ECOM Root CA 2009/7/10 DST (ABA ECO Add Trust External C Autoridad Certificador 2009/6/29 Autoridad Certifi Autoridad Certificador 2009/6/30 Autoridad Certifi Baltimore CyberTrus 2009/6/30 Autoridad Certifi Baltimore EZ by DST Baltimore EZ by DST Baltimore EZ by DST Belgacom E-Trust P	28.66	2847-44	지배마	17:3365-2:34
ABA.ECOM Root CA ABA.ECOM Root CA 2009/7/10 DST (ABA.ECO Add Trust External C Add Trust External CA 2020/5/30 USER Trust America Online Roo America Online Root 2037/11/20 America Online R Autoridad Certificad Autoridad Certificador 2009/6/29 Autoridad Certifi Autoridad Certificad Autoridad Certificador 2009/6/30 Autoridad Certifi Baltimore CyberTru Baltimore CyberTrust 2025/5/13 Baltimore Cyber Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trus 健踏(A) 健強使用目的	設備 1930-01-1-70	竣11-台 011 70	到朔日 2010 <i>月</i> 45	好記的名牌
MBA.BCOM Root CA ABA.BCOM Root CA 2009/7/10 DST (ABA.BCO ■ Add Trust External C Add Trust External CA 2020/5/30 USER Trust ■ America Online Roo America Online Root 2037/11/20 America Online R ■ Autoridad Certificad Autoridad Certificador 2009/6/29 Autoridad Certifi ■ Baltimore CyberTru Baltimore CyberTrust 2025/5/13 Baltimore Cyber ■ Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E ■ Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trus ■ Mathematica Mathematica Mathematica Prince Princ		ADA ECOM Bash CA	2012/1/12	
 Add Trust External C Add Trust External CA 2020/0/50 035EK Trust America Online Roo America Online Root 2037/11/20 America Online R Autoridad Certificad Autoridad Certificador 2009/6/29 Autoridad Certifi Baltimore CyberTru Baltimore CyberTrust 2025/5/13 Baltimore Cyber Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trust 	ABA.ECOM ROOT CA	ABA.ECOM ROOTCA	2009/7/10	DST (ABA.ECO
 Anterica Confine Root 2007/11/20 Anterica Confine R Autoridad Certificad Autoridad Certificador 2009/6/29 Autoridad Certifi Autoridad Certificad Autoridad Certificador 2009/6/30 Autoridad Certifi Baltimore CyberTru Baltimore CyberTrust 2025/5/13 Baltimore Cyber Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trust 	Muu Husi Externar C	Auto Hust External CA	2020/2/20	America Online P
 Autoridad Certificad Autoridad Certificador 2009/6/30 Autoridad Certificad Autoridad Certificador 2009/6/30 Autoridad Certificad Baltimore CyberTrust 2025/5/13 Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trust P 移除化 進階(A) 2009/2000 2009/2000 2009/2000 2009/2000 Autoridad Certifi Baltimore CyberTrust 2025/5/13 Baltimore Cyber DST (Baltimore E Belgacom E-Trust P Belgacom E-Trust P 2010/1/21 2	Millerica Onine Koo	America Omne Koor Autoridad Cartificador	2037711720 2000/6720	America Omne K
■ Ratoniam Conditional Ratoniam Conditions 2005/050 Ratoniam Conditions ■ Baltimore CyberTru Baltimore CyberTrust 2025/5/13 Baltimore Cyber ■ Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trus ■ Belgacom E-Trust P 移除 ® ● 進階(△) ● 2010/1/21 推出 ● 後除 ®	Autoridad Certificad	Autoridad Certificador	2009/0/29 2009/6/30	Autoridad Certifi
■Baltimore EZ by DST Baltimore EZ by DST 2009/7/4 DST (Baltimore E ■ Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trus ■ 匯入① 匯出 E 移除 R 進階(A) 應證使用目的	Baltimore CyberTru	Baltimore CyberTrust	2005/0/50	Baltimore Cyber
■Belgacom E-Trust P Belgacom E-Trust Pri 2010/1/21 Belgacom E-Trus 匯入① 匯出區 移除限) 進階(山) 應證使用目的 核視(V)	Baltimore EZ by DST	Baltimore EZ by DST	2009/7/4	DST (Baltimore E
▲ C C C C C C C C C C C C C C C C C C C	🔛 Belgacom E-Trust P	Belgacom E-Trust Pri	2010/1/21	Belgacom E-Trus
匯入①… 匯出 ②… 移除 ® 進階 ④… 憑證使用目的 檢視 ♡				
憑證使用目的 檢視(Y)	匯入① 匯出E)	移除(R)		道階(<u>A</u>)
檢視(♡)	憑證使用目的			
檢視♡				
				檢視(♡)
EB88 (0)				
				[闘閉C)

Mac OS) ?? ca.crt ?? Always Trust?



?? Server Certificate for Asterisk

1. ?? private key

#cd /etc/asterisk/cert

#openssl genrsa -out server.key 1024
Generating RSA private key, 1024 bit long modulus
......++++++

e is 65537 (0x10001)

2. ?? CSR (Certificate Signing Request)

#openssl req -new -key server.key -out server.csr 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) [GB]:TW

State or Province Name (full name) [Berkshire]:OSSLAb Locality Name (eg, city) [Newbury]:HC Organization Name (eg, company) [My Company Ltd]:ossLAB Organizational Unit Name (eg, section) []:OssLab Common Name (eg, your name or your server's hostname) []:alang Email Address []:

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []:

3.????

#openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt Signature ok subject=/C=TW/ST=OSSLAb/L=HC/O=ossLAB/OU=OssLab/CN=alang Getting CA Private Key Enter pass phrase for ca.key: ?? ca.key ???

?? Asterisk ????? asterisk.pem

#cd /etc/asterisk/cert
#cat server.key > asterisk.pem
#cat server.crt >> asterisk.pem
#cat asterisk.pem

asterisk.pem:

-----BEGIN RSA PRIVATE KEY-----MIICXQIBAAKBgQC0TP0bCK3RMHnqkf/VbrNzIR0Q4gSRxCjOCUHnGuPa1Y1hXV4U 0UeEgLyNPZzs2y56BXUhudgOM5U4AO+3KxlxRfycf5QFJUUmytTTtseFdX6aOHXb ... 9GxCKMrCRZAGPbo2dhyZkkc5m1WB8AHs3dJvME9nsBS/ -----END RSA PRIVATE KEY----------BEGIN CERTIFICATE-----MIIDsTCCAZkCAQEwDQYJKoZIhvcNAQEFBQAwYTELMAkGA1UEBhMCVFcxCzAJBgNV BAgTAlRXMQswCQYDVQQHEwJIQzEPMA0GA1UEChMGT1NTTGFiMQ8wDQYDVQQLEwZv ... Ae4tAwLILAWHsnJLyw3wkJW4fOtX4M5+Td2tnR6GkbobXeK63Q==

-----END CERTIFICATE-----

?? Asterisk

FreePBX > Tools > Config Edit > sip_general_custom.conf

tlsenable=yes tlsbindaddr=0.0.0.0 tlscertfile=/etc/asterisk/cert/asterisk.pem

FreePBX > Tools > Config Edit > sip_custom_post.conf

[100](+) transport=tls

Notes:

?? Asterisk ??

???? Asterisk ?? TLS????? TCP 5061 port

#netsta	at -lt					
Active	Inte	rnet connections (or	nly servers)			
Proto Recv-Q Send-Q Local Address			Foreign Address		State	
tcp	0	0 *:sip-tls	*.*	LISTEN	<=====	
tcp	0	0 *:etlservicemgr	*.*	LIST	EN	
tcp	0	0 *:mysql	*.*	LISTEN		
tcp	0	0 *:5038	*.*	LISTEN		

tcp	0	0 *:sunrpc	*.*	LISTEN
tcp	0	0 *:sieve	*.*	LISTEN
tcp	0	0 *:h323hostcall	*.*	LISTEN
tcp	0	0 pbx.local:smtp	*.*	LISTEN
tcp	0	0 *:upnotifyp	*.*	LISTEN
tcp	0	0 *:http	*.*	LISTEN
tcp	0	0 *:ssh	*.*	LISTEN
tcp	0	0 *:glrpc	*.*	LISTEN
tcp	0	0 *:paragent	*.*	LISTEN

????? TLS ??

asterisk -rx "sip show peer 100" ... Prim.Transp. : TLS Allowed.Trsp : TLS ... Reg. Contact : sip:100@123.123.123.54497;transport=TLS;rinstance=f4a38bde389d7620 ...

????? Iptables (?? PIAF ??)

?? /etc/sysconfig/iptables?????

Allow TLS connections to our SIP server -A INPUT -p tcp -m tcp --dport 5061 -j ACCEPT

?? iptables

services iptables restart

- Eyebeam 1.5+ (??? X-Lite ???)
- Blink
- 3CX Phone

Eyebeam 1.5) SIP Account Setting > Add > Account

> Display Name = User Name = Password = Domain = 123.123.123.123: 5061

> Security

Signaling Transport = TLS

Media Encryption : ?????

- Make and accept only encrypted calls (Asterisk ???? SRTP)
- Prefer to make and accept encrypted calls (Asterisk ???? SRTP)
- Make unencrypted calls, accept all calls
- Do not allow encrypted calls

??Eyebeam ????? Windows ??

3CX Phone)

Connection > New > Credentials >

> Extension: 100 ID: 100 Password: ????

My Location >

I am in the office - local IP : 123.123.123.123:5061 *??* ???????

Advanced Settings >

SIP transport: TLS *??* Certificates: ?????????? ca.crt ?? root_cert_.pem RTP mode: Normal (?? Asterisk ?? SRTP????? only secure)

?????????? TLS ??

#asterisk -rx "sip show tcp"HostPort TransportType222.222.222.22253483 TLSServer

?? SRTP ??

??? Asterisk ????res_srtp

?? SRTP
?? sip.conf

[malcolm] type=peer secret=malcolm ;note that this is NOT a secure password host=dynamic context=local dtmfmode=rfc2833 disallow=all allow=g722 transport=tls encryption=yes <==== ?? context=local

FAQ

Q: Eyebeam ??? TLS???? Service Unavailable Ans: ?? Asterisk ? TLS ????????????

Q: Command-Line ??????????

Ans:

// for *.crt
openssl x509 -noout -text -in ca.crt
// for *.csr
openssl req -noout -text -in server.csr

????

- PIAF: <u>Securing Conversations with TLS and SRTP</u>
- <u>SIPS on Asterisk SIP security with TLS</u>
- [Digium] Secure Calling Tutorial
- [Digium] Asterisk SIP/TLS Transport