?? 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 req -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:

? Common Name ??????????????????IP??

? ????? ca.crt ????????????? (self-signed) ???????????????? VeriSign?

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

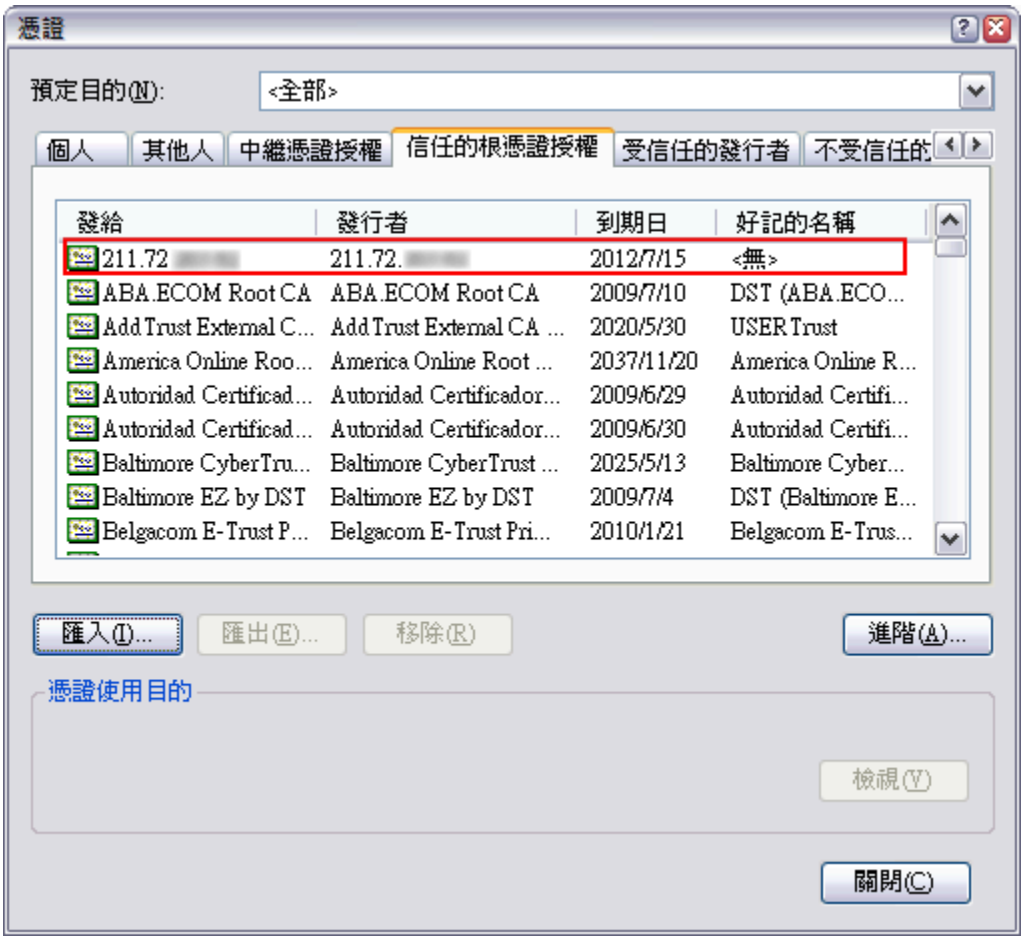
? ??? ca.crt ?????????? 365 ????????????????

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

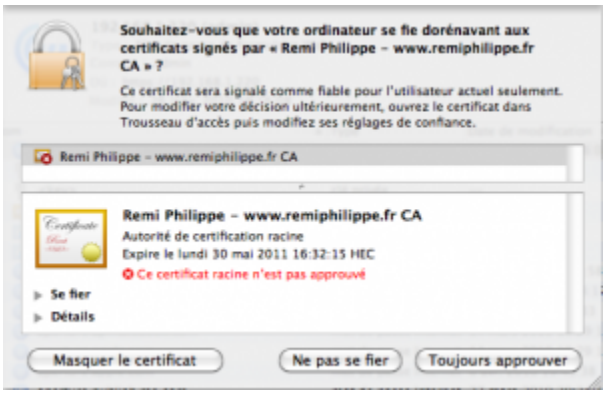
Windows XP)
??? > ?????? > ?? > ?? > ??

1. ?? ca.crt ?????
2. ??????????????? (*??*)
3. ????

??? ca.crt ????????? **????????** ?????????????



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:

- ? 100 ??????????? FreePBX ????????? TLS?????????? TLS?
- ? ??????? TLS ???????????????
- ? ??????????????????

?? Asterisk ??

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

```
#netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:sip-tls               *:*                     LISTEN   <=====
tcp        0      0 *:etlservicemgr         *:*                     LISTEN
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@123.123.123.123:54497;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
```

??????????

????????????????????? TLS ?SRTP?
????????????

- 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"
Host Port Transport Type
222.222.222.222 53483 TLS Server

?? SRTP ??

??? Asterisk ????res_srtp

??????????????? libsrtp?????? Asterisk?

?? 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: Eyebeam ??? TLS???? Certificate Validate Failure

Ans: ????????????????

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

Ans:

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

????

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