1。 证书制作

Asterisk-the_Definitive_Guide_4th_Edition[Asterisk权威文档(第4版)].pdf P177 页有使用说明

```
$ cd contrib/scripts
$ mkdir certs
$ ./ast_tls_cert -d certs -C serverA -o serverA
$ ./ast_tls_cert -d certs -C serverB -o serverB -c certs/ca.crt -k certs/ca.key
$ ls certs
ca.cfg  ca.crt  ca.key  serverA.crt  serverA.csr  serverA.key  serverA.pem
serverB.crt  serverB.csr  serverB.key  serverB.pem  tmp.cfg
```

OPTIONS:

-h Show this message

-m Type of cert "client" or "server". Defaults to server.

-f Config filename (openssl config file format)

-c CA cert filename (creates new CA cert/key as ca.crt/ca.key if not passed)

-k CA key filename

-C Common name (cert field)

This should be the fully qualified domain name or IP address for the client or server. Make sure your certs have unique common names.

-O Org name (cert field)

An informational string (company name)

-o Output filename base (defaults to asterisk)

-d Output directory (defaults to the current directory)

Example:

To create a CA and a server (pbx.mycompany.com) cert with output in /tmp:

ast_tls_cert -C pbx.mycompany.com -O "My Company" -d /tmp

This will create a CA cert and key as well as asterisk.pem and the the two files that it is made from: asterisk.crt and asterisk.key. Copy asterisk.pem and ca.crt somewhere (like /etc/asterisk) and set tlscertfile=/etc/asterisk.pem and tlscafile=/etc/ca.crt. Since this is a self-signed key, many devices will

require you to import the ca.crt file as a trusted cert.

To create a client cert using the CA cert created by the example above:

```
ast_tls_cert -m client -c /tmp/ca.crt -k /tmp/ca.key -C phone1.mycompany.com \
  -O "My Company" -d /tmp -o joe_user
```

This will create client.crt/key/pem in /tmp. Use this if your device supports
a client certificate. Make sure that you have the ca.crt file set up as
a tlscafile in the necessary Asterisk configs. Make backups of all .key files
in case you need them later.
You have new mail in /var/spool/mail/root

(1) 路径 terisk-1.8.18.0/contrib/scripts

(2) ./ast_tls_cert -d certs -C asterisk -o asterisk

在目录cert下， 生成 asterisk.pem, ca.crt, ca.key

sip.conf 设置

```
tlsenable = yes   ; Enable se
tlsbindaddr = 0.0.0.0   ; IP
; Optionally add a port numb
```

```
;
;------------------------ TLS settings ------------------------
tlscertfile = /etc/asterisk/keys/asterisk.pem ; Certificate fi
; default is to look for "asterisk.pem" in current directory

;tlsprivatekey=</path/to/private.pem> ; Private key file (*.pem
; If no tlsprivatekey is specified, tlscertfile is searched for
; for both public and private key.

tlscafile = /etc/asterisk/keys/ca.crt
;         If the server your connecting to uses a self signed ce
;         you should have their certificate installed here so th
;         verify the authenticity of their certificate.

tlscapath = /etc/asterisk/keys/
subscribecontext = default
```

对应的账号， 使能TLS

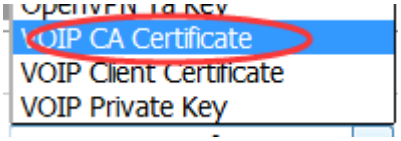
```
; then UDPTL will flow to t
[8000]
type = friend
secret = 8000
host = dynamic
transport = udp,tcp,tls
context = sunyg

[8001]
type = friend
secret = 8001
host = dynamic
transport = udp,tcp,tls
context = sunyg
```

(3) 生成 设备的证书，key

./ast_tls_cert -d certs -C device -o device -c cert/ca.crt -k cert/ca.key

在目录生成 device.pem, device.key

voip CA certificate <=>ca.crt



VOIP client Certificate <=> device.pem

VOIP Private key <=> device.key

key: 1234