Soluciones Tecnicas Alfio

- Altice trunk por internet

Altice trunk por internet

Configuración de SIP TLS con certificado privado en Issabel/Asterisk para Altice

Tutorial reproducible: Root CA privada, certificado de PBX con IP pública en Common Name y configuración de chan_sip

Resultado esperado: La PBX presenta un certificado firmado por una Root CA privada. La IP pública del cliente aparece exclusivamente en el Subject Common Name (CN), sin Subject Alternative Name (SAN). Altice importa la Root CA como autoridad confiable.

Compatibilidad: Procedimiento validado para Issabel con Asterisk 11 y chan_sip. En PJSIP los nombres de parámetros y archivos de configuración son diferentes.

1. Alcance y arquitectura

El procedimiento crea una infraestructura de certificados independiente para cada cliente. No se debe reutilizar la Root CA de otro cliente.

Dato	Valor / descripción
Root CA privada	Firma el certificado de la PBX. Altice importa únicamente el certificado público de esta CA.
Certificado de la PBX	Contiene la IP pública en el Subject CN y se presenta durante el handshake TLS.
Clave privada de la PBX	Permanece únicamente en la PBX. Nunca se comparte.
Archivo PEM	Contiene la clave privada y el certificado de la PBX para que chan_sip pueda cargarlo.

2. Datos requeridos

- IP pública de la nueva PBX.
- IP o FQDN del SBC de Altice.

- Puerto TLS asignado por Altice, normalmente 5061.
- Codecs y parámetros SIP entregados por Altice.

Ejemplo del tutorial: Se utilizará 200.10.20.30 como IP ficticia. Sustituirla por la IP pública real del cliente.

3. Respaldar la configuración existente

```
FECHA=$(date +%F-%H%M%S)
mkdir -p /root/backup-tls-$FECHA

cp -a /var/lib/asterisk/keys /root/backup-tls-$FECHA/
cp -a /etc/asterisk/sip_general_custom.conf /root/backup-tls-$FECHA/ 2>/dev/null

ls -lah /root/backup-tls-$FECHA
```

4. Crear el directorio de trabajo y definir la IP

```
mkdir -p /root/issabelpbx-certificados
cd /root/issabelpbx-certificados

IP_PUBLICA="200.10.20.30"
echo "$IP_PUBLICA"
```

5. Crear la Root CA

5.1 Generar la clave privada de la Root CA

```
openssl genrsa -out issabelpbx-root-ca.key 4096
chmod 600 issabelpbx-root-ca.key
```

Seguridad: issabelpbx-root-ca.key es la clave privada de la CA. No se envía a Altice, no se coloca en correos y debe conservarse en un respaldo seguro.

5.2 Crear la configuración de la Root CA

```
cat > issabelpbx-root-ca.cnf <<'EOF'
[req]
prompt = no
default_md = sha256
distinguished_name = dn
x509_extensions = v3_ca

[dn]
C = DO
O = IssabelPBX
OU = Voice Security
CN = IssabelPBX Root CA

[v3_ca]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical,CA:TRUE
keyUsage = critical,keyCertSign,cRLSign
EOF
```

5.3 Generar el certificado Root CA

```
openssl req -x509 -new -key issabelpbx-root-ca.key -sha256 -days 3650 -out issabelpbx-root-ca.crt -config issabelpbx-root-ca.cnf
```

5.4 Verificar la Root CA

```
openssl x509 -in issabelpbx-root-ca.crt -noout -subject -issuer -dates

openssl x509 -in issabelpbx-root-ca.crt -noout -text | grep -A3 "Basic Constraints"
```

Resultado esperado: el Subject y el Issuer son iguales y aparece CA:TRUE.

6. Crear el certificado de la PBX

6.1 Generar la clave privada de la PBX

```
openssl genrsa -out issabelpbx.key 2048
chmod 600 issabelpbx.key
```

Compatibilidad: RSA 2048 ofrece mayor compatibilidad con SBC antiguos. Si Altice confirma soporte y existe un requerimiento formal, puede usarse RSA 4096.

6.2 Crear la configuración con la IP en el Common Name y sin SAN

```
cat > issabelpbx.cnf <<EOF
[req]
prompt = no
default_md = sha256
distinguished_name = dn

[dn]
C = DO
O = IssabelPBX
OU = VoIP
CN = ${IP_PUBLICA}

[v3_cert]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
basicConstraints = critical,CA:FALSE
keyUsage = critical,digitalSignature,keyEncipherment
extendedKeyUsage = serverAuth,clientAuth
EOF
```

Requisito de Altice: No agregar subjectAltName. La IP debe quedar exclusivamente en Subject Common Name (CN).

6.3 Generar el CSR

```
openssl req -new -key issabelpbx.key -out issabelpbx.csr -config issabelpbx.cnf

openssl req -in issabelpbx.csr -noout -subject
```

Resultado esperado: CN=IP_PUBLICA.

6.4 Firmar el certificado con la Root CA

```
openssl x509 -req -in issabelpbx.csr -CA issabelpbx-root-ca.crt -CAkey issabelpbx-root-ca.key -CAcreateserial -out issabelpbx.crt -days 825 -sha256 -extfile issabelpbx.cnf -extensions v3_cert
```

6.5 Crear el PEM que utilizará Asterisk

```
cat issabelpbx.key issabelpbx.crt > issabelpbx.pem
chmod 600 issabelpbx.pem

grep "BEGIN" issabelpbx.pem
```

Debe aparecer una clave privada y un certificado.

7. Validar los certificados antes de instalarlos

7.1 Verificar Subject, Issuer, vigencia y serie

```
openssl x509 -in issabelpbx.crt -noout -subject -issuer -dates -serial -fingerprint -sha256
```

Debe mostrarse el CN con la IP pública y el Issuer como IssabelPBX Root CA.

7.2 Confirmar que no existe SAN

```
openssl x509 -in issabelpbx.crt -noout -text | grep -A3 "Subject Alternative Name"
```

El comando no debe devolver ninguna línea.

7.3 Verificar la cadena de confianza

```
openssl verify -CAfile issabelpbx-root-ca.crt issabelpbx.crt
```

Resultado esperado: issabelpbx.crt: OK

7.4 Verificar que la clave y el certificado coincidan

```
openssl x509 -in issabelpbx.crt -noout -modulus | openssl md5
openssl rsa -in issabelpbx.key -noout -modulus | openssl md5
```

Los dos hashes deben ser idénticos.

8. Archivos generados y tratamiento

Archivo	Función	¿Se comparte con Altice?
issabelpbx-root-ca.crt	Certificado público de la Root CA	Sí
issabelpbx-root-ca.key	Clave privada de la Root CA	Nunca
issabelpbx.crt	Certificado público de la PBX	Solo si Altice lo solicita
issabelpbx.key	Clave privada de la PBX	Nunca
issabelpbx.pem	Clave privada + certificado para Asterisk	Nunca
issabelpbx.csr	Solicitud de certificado	No es necesario

Entrega habitual: Altice importa issabelpbx-root-ca.crt como Trusted Root CA. La PBX presenta issabelpbx.crt automáticamente durante el handshake TLS.

9. Instalar los certificados en Issabel

```
cp /root/issabelpbx-certificados/issabelpbx.pem /var/lib/asterisk/keys/

cp /root/issabelpbx-certificados/issabelpbx.crt /var/lib/asterisk/keys/

cp /root/issabelpbx-certificados/issabelpbx-root-ca.crt /var/lib/asterisk/keys/

chown asterisk:asterisk /var/lib/asterisk/keys/issabelpbx.pem /var/lib/asterisk/keys/issabelpbx.crt
/var/lib/asterisk/keys/issabelpbx-root-ca.crt

chmod 640 /var/lib/asterisk/keys/issabelpbx.pem
chmod 644 /var/lib/asterisk/keys/issabelpbx.crt
chmod 644 /var/lib/asterisk/keys/issabelpbx-root-ca.crt
```

10. Configurar TLS en chan_sip

Editar /etc/asterisk/sip_general_custom.conf y agregar o ajustar:

```
tlsenable=yes
tlsbindaddr=0.0.0.0:5061
tlsclientmethod=tlsv1_2
tlsdontverifyserver=yes
tlscertfile=/var/lib/asterisk/keys/issabelpbx.pem
tlscafile=/var/lib/asterisk/keys/issabelpbx-root-ca.crt
```

Importante: tlsdontverifyserver=yes desactiva la validación del certificado remoto por parte de la PBX. No afecta la validación que Altice realiza sobre el certificado de la PBX.

Buscar configuraciones TLS duplicadas:

```
grep -RniE '^(tlsenable|tlsbindaddr|tlsclientmethod|tlsdontverifyserver|tlscertfile|tlscafile)' /etc/asterisk
```

11. Configurar el trunk de Altice

Plantilla: Los parámetros de autenticación, dominio, DID, codecs y SRTP deben ajustarse a la ficha técnica entregada por Altice.

```
type=peer
host=IP_SBC_ALTICE
port=5061
transport=tls
context=from-trunk
disallow=all
allow=ulaw
allow=alaw
insecure=port,invite
qualify=yes

; Si Altice exige SRTP:
; encryption=yes
```

12. Reiniciar y verificar Asterisk

```
systemctl restart asterisk
systemctl status asterisk --no-pager

asterisk -rx "sip show settings" | grep -i -A5 TLS
ss -lntp | grep 5061
```

Debe aparecer TLS SIP Bindaddress: 0.0.0.0:5061 y Asterisk escuchando en el puerto TCP 5061.

13. Confirmar el certificado realmente presentado por Asterisk

```
echo | openssl s_client -connect 127.0.0.1:5061 -showcerts 2>/dev/null | openssl x509 -noout -subject -issuer -dates -serial -fingerprint -sha256
```

La salida debe mostrar Subject CN=IP_PUBLICA e Issuer CN=IssabelPBX Root CA.

```
echo | openssl s_client -connect 127.0.0.1:5061 -showcerts 2>/dev/null | openssl x509 -noout -text | grep -A3 "Subject Alternative Name"
```

No debe mostrar resultados.

14. Verificación externa y captura con Wireshark

Desde una red externa, probar el puerto y el certificado:

```
openssl s_client -connect IP_PUBLICA:5061 -tls1_2 -showcerts
```

En Wireshark puede filtrarse el certificado con:

```
tls.handshake.type == 11
```

En versiones antiguas:

```
ssl.handshake.type == 11
```

Ruta de validación: TLS > Handshake Protocol: Certificate > Certificate > signedCertificate > subject > commonName. Debe aparecer la IP pública.

15. Errores frecuentes y diagnóstico

Mensaje	Interpretación probable	Acción recomendada
tlsv1 alert unknown ca	El SBC no confía en la CA emisora.	Confirmar que Altice importó issabelpbx-root-ca.crt como Trusted Root CA y lo asoció al trunk.
tlsv1 alert internal error	El SBC superó o cambió la etapa de validación, pero falla otra política.	Revisar CN, ausencia de SAN, RSA 2048/4096, EKU, TLS 1.2, cifrados y logs detallados del SBC.
FILE * open failed!	Asterisk no pudo completar o manejar el flujo TLS, o no puede leer un archivo.	Validar rutas, permisos, propietario y el error TLS inmediatamente anterior.

Mensaje	Interpretación probable	Acción recomendada
Asterisk presenta un certificado antiguo	La configuración no fue recargada o existe otra definición TLS.	Revisar grep recursivo, reiniciar Asterisk y repetir openssl s_client contra 127.0.0.1:5061.
No aparece CN con la IP	Se generó el certificado con otro Subject.	Recrear el CSR y certificado verificando CN=${IP_PUBLICA}.
Aparece Subject Alternative Name	La plantilla incluyó SAN.	Regenerar el certificado sin ninguna sección subjectAltName.

16. Lista de comprobación final

☐ Se creó una Root CA exclusiva para el cliente.

☐ La Root CA muestra CA:TRUE.

☐ El certificado de la PBX muestra CA:FALSE.

☐ El Subject CN contiene la IP pública correcta.

☐ El certificado no contiene Subject Alternative Name.

☐ Extended Key Usage incluye serverAuth y clientAuth.

☐ openssl verify devuelve OK.

☐ La clave privada coincide con el certificado.

☐ El PEM contiene la clave privada y el certificado.

☐ Los archivos están instalados en /var/lib/asterisk/keys.

☐ Los permisos y propietario son correctos.

☐ Asterisk escucha en TCP 5061.

☐ El trunk utiliza transport=tls.

☐ Altice importó la Root CA.

☐ openssl s_client confirma el certificado activo.

☐ Wireshark muestra la IP en subject > commonName.

17. Respaldo recomendado

```
mkdir -p /root/respaldo-pki-issabelpbx
cp -a /root/issabelpbx-certificados/* /root/respaldo-pki-issabelpbx/
chmod 700 /root/respaldo-pki-issabelpbx
chmod 600 /root/respaldo-pki-issabelpbx/*.key
```

Conservación: Guardar una copia cifrada y fuera del servidor de issabelpbx-root-ca.key. Sin esa clave no será posible emitir nuevos certificados bajo la misma Root CA.

18. Resumen operativo

1. Crear una Root CA nueva y exclusiva para el cliente.
2. Crear la clave y el CSR de la PBX con la IP pública en CN y sin SAN.
3. Firmar el certificado de la PBX con la Root CA.
4. Validar cadena, CN, ausencia de SAN y coincidencia de clave.
5. Enviar a Altice únicamente el certificado público de la Root CA, salvo que soliciten otro archivo.
6. Instalar PEM, certificado y Root CA en Issabel.
7. Configurar chan_sip, trunk TLS y reiniciar Asterisk.
8. Verificar el certificado activo con openssl s_client y, si es necesario, con Wireshark.