

## ANNEXE

### Document 1 – Présentation du chiffrement

L'écoute des messages est rendue possible par le positionnement MITM et l'utilisation de comptes non chiffrés. Le chiffrement n'évitera pas l'empoisonnement ARP mais rendra impossible l'écoute des messages. Deux éléments sont à considérer :

- -le chiffrement du flux associé à la signalisation. Il s'agit des messages échangés dans le cadre du protocole SIP, c'est à dire l'authentification du client et la préparation de l'appel.
- -le chiffrement du transport de la voix. Il s'agit de la voix transportée par le protocole RTP.

La configuration du chiffrement des échanges nécessite de créer des certificats sur le serveur et de préparer les téléphones pour des échanges à travers le protocole TLS.



Attention, l'utilisation d'un softphone pour le chiffrement nécessite de vérifier qu'il est compatible avec la configuration TLS. Le logiciel Blink est un bon candidat en la matière.

### Document 2 - Installation de Blink

Vous trouverez le fichier d'installation du client Blink pour Windows en suivant ce lien :

<https://blink.sipthor.net/download.phtml?download&os=nt>

## Document 3 - Configuration TLS du serveur Asterisk

Il faut créer des certificats signés par notre autorité de certification. Le paquet `openssl` permet l'utilisation des commandes permettant de créer ces fichiers.

Le paquet `srtplib` permet de configurer le chiffrement du flux associé au transport de la voix.

```
#apt-get install openssl srtplib
```

### D3.1 - Modification du fichier `sip.conf`

Dans le fichier `sip.conf`, il faut ajouter les deux lignes suivantes pour chaque utilisateur concerné par le chiffrement.

```
[John]
...
transport = tls
encryption = yes
```

### D3.2 - Création des certificats

Par défaut la communication se fait avec le protocole UDP via le port 5060. L'activation de TLS va permettre l'utilisation du port 5061 via le protocole TCP. Plusieurs étapes sont nécessaires pour créer les certificats afin d'obtenir l'exemple d'arborescence figurant dans la capture d'écran ci-dessous. (Attention, dans la capture d'écran, les utilisateurs se nomment 'utilisateur1' et 'utilisateur2', ce n'est pas le cas dans votre plateforme de tests.

```
root@asterisk:/etc/asterisk/certificats# ls -R
.:
ca  srv  utilisateur1  utilisateur2

./ca:
ca.crt  ca.key

./srv:
asterisk.pem  key.pem  req-srv.csr  srv.crt

./utilisateur1:
cert-utilisateur1.crt  cert-utilisateur1.pem  key.pem  req-utilisateur1.csr

./utilisateur2:
cert-utilisateur2.crt  cert-utilisateur2.pem  req-utilisateur2.csr
cert-utilisateur2.pem  key.pem
```

#### → Création du certificat de l'autorité de certification

Dans le répertoire **ca** :

L'autorité de certification devra signer les certificats générés.

Création de la clé :

```
#openssl genrsa -des3 -out ca.key 4096
```

Une **passphrase** est demandée lors de création du certificat.

Création du certificat :

```
#openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

## → Création du certificat du serveur Asterisk

Dans le répertoire **srv** :

Création de la clé :

```
#openssl genrsa -out key.pem 1024
```

Création du fichier de demande de certificat :

```
#openssl req -new -key key.pem -out req-srv.csr
```

Création du certificat :

```
openssl x509 -req -days 365 -in req-srv.csr -CA ../ca/ca.crt -CAkey ../ca/ca.key -set_serial 01 -out srv.crt
```

Les fichiers *.pem* et *.crt* peuvent être mis dans un seul fichier *.pem* qui contiendra ainsi la clé et le certificat.

```
#cat key.pem > asterisk.pem
```

```
#cat srv.crt >> asterisk.pem
```

## → Création des certificats des softphones

Dans le répertoire d'un softphone (**John** par exemple) :

Il faut reproduire les étapes liées à la création du certificat du serveur en l'adaptant pour chaque utilisateur (clé, demande de certificat, certificat).

### D3.3 - Modification du fichier sip.conf

Dans le fichier sip.conf, il faut activer TLS et faire référence au certificat du serveur.

<i>tlsenable = yes</i>	<i>;active TLS</i>
<i>tlscertfile = /etc/asterisk/certificats/srv/asterisk.pem</i>	<i>;certificat du serveur</i>
<i>tlscacfile = /etc/asterisk/certificats/ca/ca.crt</i>	<i>;certificat de l'autorité</i>
	<i>;de certification</i>
<i>tlscipher = all</i>	<i>;spécifie quels algorithmes de</i>
	<i>;chiffrement sont utilisés</i>
<i>tlscclientmethod = tlsv1</i>	<i>;version de TLS supportée</i>
...	

Voici un exemple de configuration :

```
root@asterisk:/etc/asterisk# more sip.conf
[general]
context=public
transport = tls
tlsenable=yes
tlscbindaddr=0.0.0.0:5061
tlscertfile=/etc/asterisk/certificats/srv/asterisk.pem
tlscacfile=/etc/asterisk/certificats/ca/ca.crt
tlscipher=ALL
tlscclientmethod=tlsv1
tlscdontverifyserver = yes
```

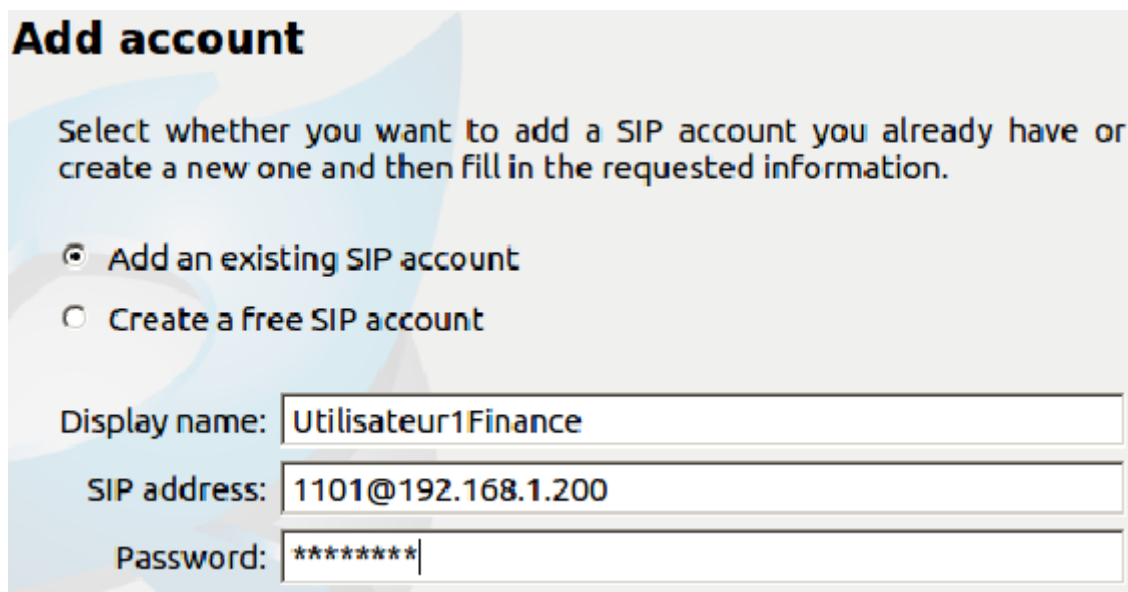
## Document 4 - Configuration des comptes TLS sur les softphones Blink

Quelques modifications sont nécessaires par rapport à un compte ne faisant pas appel au chiffrement.

### D4.1 - Création d'un compte SIP

Il faut ajouter un compte existant en indiquant le nom, la référence au serveur sous la forme **numéro-téléphone@ip-serveur** et le mot de passe. Pour cela, il faut aller dans **Blink** puis **Accounts** et sur **Manage accounts**.

Attention à adapter les captures d'écran ci-dessous à votre contexte.



**Add account**

Select whether you want to add a SIP account you already have or create a new one and then fill in the requested information.

☒ Add an existing SIP account  
☐ Create a free SIP account

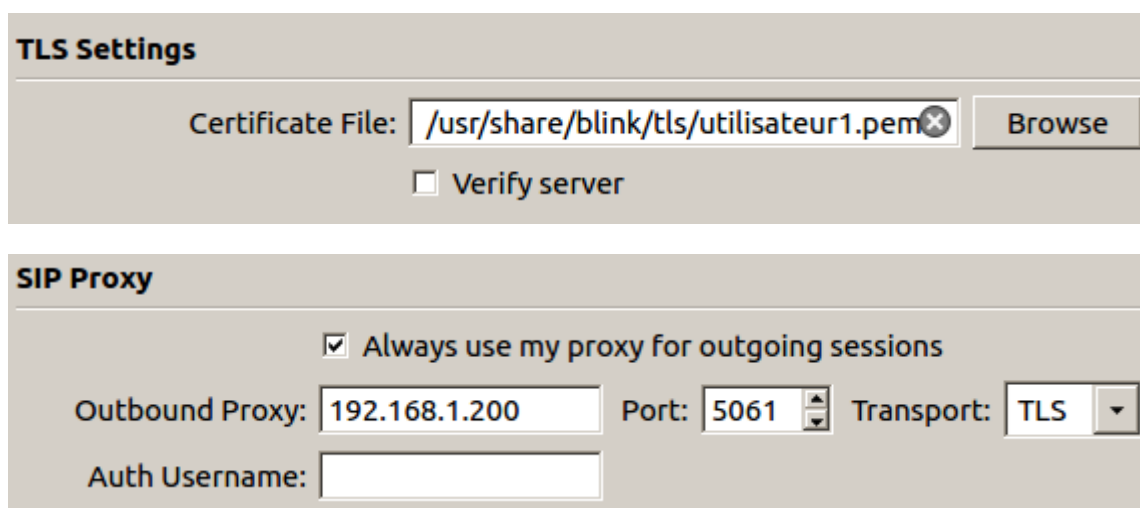
Display name:

SIP address:

Password:

### D4.2 - Configuration du chiffrement

Ensuite, il faut indiquer le fichier contenant le certificat de l'utilisateur et positionner le trafic en TLS. Les onglets **Server Settings** et **Advanced** du menu **Account** permettent d'établir ces configurations.



**TLS Settings**

Certificate File:

☐ Verify server

**SIP Proxy**

☒ Always use my proxy for outgoing sessions

Outbound Proxy:  Port:  Transport:

Auth Username:

Il faut aussi faire référence au certificat de l'autorité de certification. La configuration se trouve dans le menu **Advanced** du compte SIP.

**TLS settings**

Certificate Authority:

Pour la configuration du SRTP, il faut activer l'option **SDES mandatory** dans le menu **account/media/rtp options**.

**RTP Options**

☒ Send inband DTMF

☒ Encrypt audio and video

Encryption:

### D4.3 - Enregistrement du compte sur le serveur

Lorsque ces configurations sont terminées, la console Asterisk doit tracer l'enregistrement du softphone. Il faut être attentif à la validation du certificat. Le message **SSL certificate OK** doit apparaître. L'enregistrement fait apparaître la référence au logiciel Blink.

```
> Saved useragent "Blink 2.0.0 (Linux)" for peer 1101
> Saved useragent "Blink 2.0.0 (Linux)" for peer 1201
```

### D4.4 - Dépannages

- ❖ A la fin de l'étape du paragraphe 4.1, le serveur trace une erreur sur le mode de transport. En effet, nos comptes sont configurés en TLS sur le serveur. Or, la validation de cette première étape positionne un mode de transport par défaut en UDP. Ce n'est qu'à la fin de la configuration en TLS que le message disparaît.

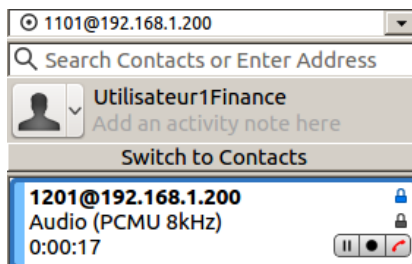
```
[Nov 11 10:45:32] ERROR[1513]: chan_sip.c:16898 register_verify: 'UDP' is not a
valid transport for '1201'. we only use 'TLS'! ending call.
```

- ❖ Dans le fichier **sip.conf**, la ligne **tlsdontverifyserver** permet de ne plus avoir le message d'erreur associé à l'utilisation d'un certificat auto-signé.

```
[Nov 11 11:03:40] ERROR[1876]: tcptls.c:621 handle_tcptls_connection: Certificat
e did not verify: self signed certificate
```

## Document 5 - Premier appel et capture de trames

Lors d'un appel, le cadenas bleu indique le chiffrement du flux de signalisation. Le cadenas gris indique le chiffrement du flux RTP. Lorsque la souris passe sur un cadenas, une explication apparaît.



Concernant le flux de signalisation, une capture avec le filtre **tcp.port == 5061** permet de constater le chiffrement TLS.

No.	Time	Source	Destination	Protocol	Length	Info
21	11.974387000	192.168.1.11	192.168.1.200	TLSv1.2	1217	Application Data
22	11.974441000	192.168.1.10	192.168.1.11	ICMP	590	Redirect (Redirect for host
23	11.974484000	192.168.1.11	192.168.1.200	TLSv1.2	1217	[TCP Retransmission] Application Data
24	11.975226000	192.168.1.200	192.168.1.11	TLSv1.2	715	Application Data
25	11.975249000	192.168.1.10	192.168.1.200	ICMP	590	Redirect (Redirect for host
26	11.975270000	192.168.1.200	192.168.1.11	TLSv1.2	715	[TCP Retransmission] Application Data
27	11.975389000	192.168.1.11	192.168.1.200	TCP	66	57727-5061 [ACK] Seq=1152 Ack=650 Win=1

Filter: tcp.port == 5061 Expression... Clear Apply Enregistrer

► Frame 26: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface 0

► Ethernet II, Src: CadmusCo\_08:cb:36 (08:00:27:08:cb:36), Dst: LiteonTe\_62:ee:fb (20:16:d8:62:ee:fb)

► Internet Protocol Version 4, Src: 192.168.1.200 (192.168.1.200), Dst: 192.168.1.11 (192.168.1.11)

► Transmission Control Protocol, Src Port: 5061 (5061), Dst Port: 57727 (57727), Seq: 1, Ack: 1152, Len: 649

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Application Data Protocol: sip.tcp

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 644

## Document 6 - Autres contre-mesures

### D6.1 - Filtrage des adresses MAC

Pour éviter en amont ce type d'attaque, une politique de filtrage des adresses MAC peut être envisagée. L'idée est d'empêcher un utilisateur de connecter son ordinateur portable au réseau. Cette connexion de périphériques non légitimes est souvent le point de départ des attaques associées aux réseaux locaux. Ce filtrage peut être mis en place sur des équipements réseaux comme les commutateurs ou les routeurs dans le cadre d'une politique de sécurisation des ports.

Le filtrage des adresses MAC présente néanmoins l'inconvénient d'alourdir l'administration du réseau. En outre, une adresse MAC peut facilement s'usurper avec l'utilisation de logiciels tel que *macchanger*.

### D6.2 - Surveillance du trafic ARP

La création d'entrées statiques dans le cache ARP peut apporter un début de réponse mais ce procédé oblige à figer une configuration.

C'est pourquoi des outils existent afin de surveiller les évolutions du cache ARP dans le but de détecter des modifications suspectes.

Le logiciel *arpwatch* assure cette fonction en surveillant l'activité ARP du réseau local.

### D6.3 - IDS/IPS

Les systèmes de détection d'intrusion (IDS) sont des dispositifs qui capturent et analysent le trafic à la recherche de trames associées à un trafic malicieux. Un mécanisme d'alerte est alors configuré afin d'avertir l'administrateur. Plusieurs solutions existent. On peut citer l'exemple du logiciel *snort*.

Les systèmes de prévention d'intrusion (IPS) sont des IDS actifs qui peuvent prendre des mesures afin de diminuer les impacts d'une attaque en bloquant des ports par exemple. Le logiciel *snort* est aussi un IPS. Des constructeurs comme CISCO ou JUNIPER sont aussi présents sur ce marché.

L'envoi continu de fausses réponses ARP est considéré comme du trafic malicieux susceptible d'être détecté par un IDS/IPS.