AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Installation du DNS (Bind9)

- Mettre à jour les paquets

```
# apt-get update
# apt-get upgrade
```

- Installation du paquet BIND9

```
# apt-get install bind9
```

- Le fichier named.conf.local : Ce fichier contient la configuration locale du serveur DNS, on y déclare les zones associées au domaine.

/etc/bind/named.conf.local

```
zone "aerodefense.stri" {
        type master;
        file "/etc/bind/db.aerodefense.stri";
        allow-query {
                any;
        };
        allow-transfer {
                172.30.0.1;
        };
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.aerodefense.stri.inv";
        allow-query {
                any;
        };
        allow-transfer {
                172.30.0.1;
        };
};
```

- Les Ressources Records (RR) : Un DNS est constitué de plusieurs enregistrements, les RR ou Ressources Records, définissant les diverses informations relatives au domaine. Le premier enregistrement est consacré à la résolution de noms, dans notre cas, il s'agit du fichier db.aerodefense.stri. Le second sera quant à lui en rapport avec la résolution de noms inverses ; il s'agit du fichier db.aerodefense.stri.inv.

/etc/bind/db.aerodefense.stri

```
$TTL  60
@       IN      SOA     zeus.aerodefense.stri. root.aerodefense.stri. (
     2006081401
     28800
     3600
     604800
     38400
 )
@       IN      A               192.168.1.1
@       IN      NS              zeus
@       IN      NS              zeus.aerodefense.stri.
@       IN      MX              10 mail
```

```
zeus                    IN      A       192.168.1.1
mail                    IN      A       192.168.1.10
localhost               IN      A       127.0.0.1

www     CNAME   zeus
smtp    CNAME   mail
pop     CNAME   mail
```

/etc/bind/db.aerodefense.stri.inv

```
$TTL 60
@       IN SOA zeus.aerodefense.stri. root.aerodefense.stri. (
                        2006081401;
                        28800;
                        604800;
                        604800;
                        86400)
                    IN    NS     zeus.aerodefense.stri.
1                   IN    PTR    zeus.aerodefense.stri.
10                  IN    PTR    mail.aerodefense.stri.
```

- Le Fichier resolv.conf

```
search aerodefense.stri
```

$TTL : (Time To Live) exprime la durée (en secondes) de validité, par défaut, des informations que contiennent les RRs. Une fois ce délai expire, il est nécessaire de revérifier les données. Les différents types:

- **SOA** : permet de définir les informations relatives à la zone. Il est compose de plusieurs champs :
    - 1. *Serial* : est un entier non signé 32 bits. C'est le numéro de série à incrémenter à chaque modification du fichier. Il permet au serveur secondaire de recharger les informations qu'ils ont. L'usage général vient à le formater de cette manière YYYYMMDDXX, soit pour la première modification du 01/10/2010 -> 2010100101, pour la seconde 2010100102.
    - 2. *Refresh* : définit la période de rafraîchissement des données.
    - 3. *Retry* : si une erreur survient au cours du dernier rafraîchissement, celle -ci sera répéter au bout du délai Retry.
    - 4. *Expire* : le serveur sera considéré comme non disponible au bout du délai Expire.
    - 5. *Negative cache TTL* : défini la durée de vie d'une réponse NXDOMAIN de notre part.
- **NS** : renseigne le nom des serveurs de noms pour le domaine.
- **MX** : renseigne sur le serveur de messagerie. Plusieurs peuvent être définis. Ainsi, il est possible de leur donner une priorité en leur affectant un numéro. Plus bas est le numéro, plus haute est la priorité.
- **A** : associe un nom d'hôte à une adresse ipv4 (32 bits)
- **AAAA** : associe un nom d'hôte à une adresse ipv6 (128 bits)
- **CNAME** : identifie le nom canonique d'un alias (un nom pointant sur un autre nom)
- **PTR** : c'est simplement la résolution inverse (le contraire du type A).

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Installation Postfix :

- Mettre à jour les paquets :

```
# apt-get update
# apt-get upgrade
```

- Installation du paquet postfix :

```
# apt-get install postfix
```

- Le fichier main.cf : Ce fichier renseigne un petit sous-ensemble des paramètres qui contrôlent les opérations du système de messagerie Postfix.

/etc/postfix# vim main.cf

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no

smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noanonymous
smtp_always_send_ehlo = yes

myhostname = zeus.aerodefense.stri
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydomain = aerodefense.stri
myorigin = /etc/mailname
mydestination = mail.aerodefense.stri, zeus.aerodefense.stri,
localhost.aerodefense.stri, aerodefense.stri, localhost.localdomain, localhost
relayhost = smtp.cict.fr
mynetworks = 127.0.0.0/8
inet_interfaces = all
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = loopback-only
default_transport = error
relay_transport = error
```

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Installation Spamassassin

```
apt-get install spamassassin spamc
```

- Quelques opérations système sont nécessaires pour installer spamassassin avec postfix (en root)

```
# groupadd spamd
# useradd -g spamd -s /bin/false -d /var/log/spamassassin spamd
# mkdir /var/log/spamassassin
# chown spamd:spamd /var/log/spamassassin
```

- Configuration de Spamassassin

Edit /etc/default/spamassassin

```
# Change to one to enable spamd
ENABLED=1
SAHOME="/var/lib/spamassassin/"

# Options
# See man spamd for possible options. The -d option is automatically added.

# SpamAssassin uses a preforking model, so be careful! You need to
# make sure --max-children is not set to anything higher than 5,
# unless you know what you're doing.

OPTIONS="--create-prefs --max-children 5 --username spamd --helper-home-dir
${SAHOME} -s ${SAHOME}spamd.log"
```

- Start Spamassassin daemon (spamd)

```
/etc/init.d/spamassassin start
```

- Configuration de Postfix pourqu'il utilise Spamassassin comme un filtre

/etc/postfix/master.cf

```
smtp      inet  n       -       -       -       -       smtpd  -v
        -o content_filter=spamassassin

spamassassin unix -     n       n       -       -       pipe
        user=spamd argv=/usr/bin/spamc -f -e
        /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

- Pour entrainer le filtre sur ce que le junk ressemble à :

```
sudo sa-learn --spam -u spamd --dir /home/ell/Maildir/.Junk/* -D
```

- Et ce que le non-spam ressemble à :

```
sudo sa-learn --ham -u spamd --dir /home/ell/Maildir/.INBOX/* -D
```

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Installation squirrelmail

```
#aptitude install apache2
#aptitude install libapache2-mod-php5 php5-cli php5-common php5-cgi
#aptitude install squirrelmail
```

- Modification de apache2.conf

/etc/apache2/apache2.conf

```
Include /etc/squirrelmail/apache.conf
/etc/init.d/apache2 restart
```

- Edition minimum de config.php

/etc/squirrelmail/config.php

```
$org_name = "Aerodefense";
$domain ='zeus.aerodefense.stri';
$smtpServerAddress = 'localhost';
$imapServerAddress = 'localhost';
$imap_server_type = 'uw';
$use_imap_tls = true;
$imap_auth_mech = 'login';
$imapPort = 993;
```

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Installation de PHP

- Mettre à jour les paquets :

```
apt-get update
```

- Installation du paquet PHP :

```
apt-get install libapache2-mod-php5
```

- Configuration des options :

```
/etc/php5/apache2/php.ini
```

    - display_errors = Off
    - log_errors = On
    - Upload de fichiers
    - file_uploads = On
    - upload_max_filesize = 8M
    - max_execution_time = 60
    - register_globals off
    - safe_mode = Off
    - allow_url_fopen = off
    - log_errors On
    - display_errors Off
    - error_log /var/log/php/errors
- Redémarrer le serveur apache

```
apache2 -k restart
```

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Installation de MySQL

- Installation

```
apt-get install mysql-server
apt-get install php5-mysql
```

- Configuration

    - Changer le mot de passe

```
mysql
use mysql
UPDATE user SET password = PASSWORD('VOTREPASSMYSQL') WHERE user = 'root';
flush privileges;
quit
```

    - Supprimer Utilisateurs vides :

```
DELETE FROM mysql.user WHERE User='';
FLUSH PRIVILEGES;
```

    - Supprimer Table de test :

```
DROP DATABASE test;
DELETE FROM mysql.db WHERE Db='test' OR Db='test\_%';
```

Guide d'installation

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Configuration de Thunderbird pour la gestion des signatures + cryptage.

Date de création	25/10/2010		
Auteur(s) du document	Wannes VOSSEN	**Version actuelle**	1.0
Approbateur(s) du document		**Date Approbation**	

Historique des versions			
Version	**Date**	**Auteur modif.**	**Notes**
1.0	25/10/2010	Wannes	Création du document.

Sommaire

Guide d'installation

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

I - Principe de fonctionnement

1 - Cryptage

Vous allez être emmenés à créer, à l'aide de serveur dédiés, un système de chiffrement pour vos communications. Ce système se constitue de deux clés :

- Une clé Publique.
- Une clé Privée.

La Clé publique peut et doit être communiqué à vos destinataires. Elle permettra à quiconque de crypter les messages qui vous sont destinés. Seule votre clé Privée permet de décrypter un message qui aurait été crypté à l'aide de votre clé publique : La clé privé doit être gardée secrète.

2 - Signature

Le système de signature des messages recoure à un tiers de confiance pour authentifier l'émetteur d'un message.

II - Installations logicielles

La mise en œuvre du cryptage et de la signature des emails nécessite l'installation préalable des logiciels suivants :

- Mozilla Thunderbird (http://www.mozillamessaging.com/fr/thunderbird/).
- GnuPG (http://www.gnupg.org/download/).
- Plugin Enigmail pour Mozilla Thunderbird (http://enigmail.mozdev.org/download/index.php.htm).

Remarque : Veillez à bien autoriser Thunderbird et l'ensemble des exécutables de GnuPG au travers de votre pare-feu.

III - Mise en place du système

1 - Récupération et mise à disposition des clés publiques

Il existe deux méthodes pour récupérer les clés publiques de vos correspondants et mettre les vôtres à disposition :

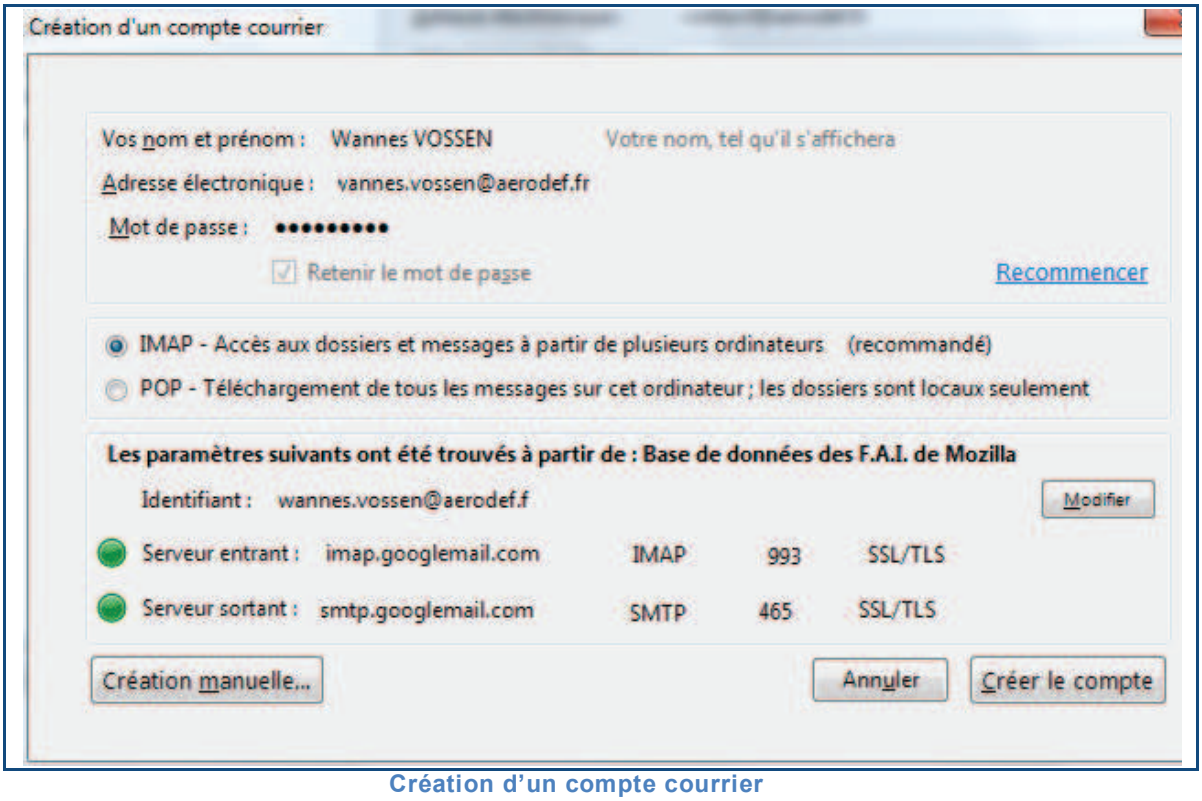
- La clé peut être envoyée directement par email sous forme d'un fichier joint. Dans ce cas, le premier échange est forcément non-crypté.
- La clé peut être envoyée à un serveur de clés. Elle sera alors associée à une adresse email et tout un chacun pourra la récupérer.

Certaines clés publiques qui ont déjà été échangées avec le groupe Audit se trouvent sur Google Docs, dossier communication.

2 - Configuration du compte AeroDef.fr dans Thunderbird

Pour configurer un nouveau compte @aerodef.fr en IMAP, suivez les instructions suivantes :

- Cliquez Outils -> Paramètres des Comptes -> Gestion des comptes -> Ajouter un nouveau compte de messagerie.



Création d'un compte courrier

Thunderbird devrait trouver seul les paramètres de configuration. Autrement, renseignez ceux figurant sur la capture ci-dessus.

3 - Configuration de OpenPGP dans Thunderbird

1.3 - Assistant de configuration

Pour ce faire, nous utiliserons l'assistant de configuration. Dans Thunderbird, cliquez :

- OpenPGP -> Assistant de configuration OpenPGP.
- Sélectionnez « Oui je souhaite que l'assistant m'aide à démarrer ».
- Configurer OpenPGP pour les identités suivantes seulement : votre identité @aerodef.fr.
- Au choix, signez tous vos messages ou non.
- Répondez non merci quand on vous demande si vous voulez qu'Enigmail reconfigure Thunderbird.
- Cliquez enfin « Créer une clé pour chiffrer et signer vos messages ».

2.3 - Gestion des clés

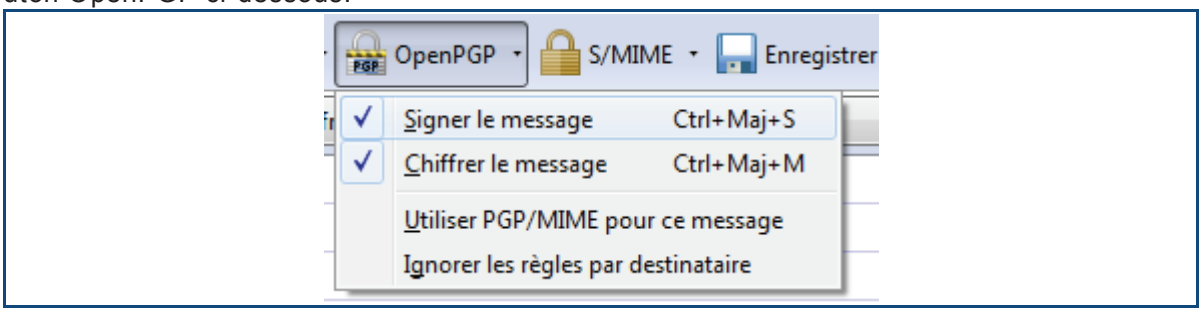
OpenPGP est maintenant prêt à l'emploi. Voyons les manipulations possibles concernant la gestion des clés publiques et privées. Cliquez : OpenPGP -> Gestion des clés.

Dans la fenêtre de gestion des clés, vous pouvez entre autre :

- Exporter vos clés publiques et/ou privées vers un fichier : Clic droit -> Exporter les clés vers un fichier.
- Publier votre clé publique sur un serveur de clés pour la mettre à disposition des autres : Clic droit -> Envoyer les clefs publiques vers un serveur de clefs.
- Augmenter le niveau de confiance d'une clé. Cela permet d'éviter les demandes de confirmation lors de l'envoi de messages cryptés et/ou signés : Clic droit -> augmenter le niveau de confiance du destinataire.

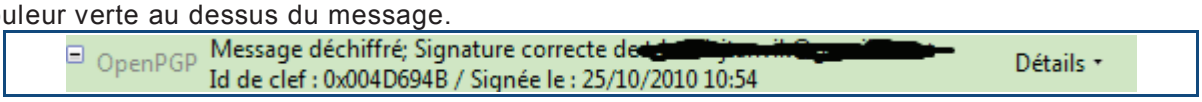
4 - Envoi d'un message crypté et signé

Pour envoyer un message crypté, composez votre email à l'aide de Thunderbird et utilisez le bouton OpenPGP ci-dessous.



5 - Vérification de la signature d'un message

Lorsqu'un message est correctement signé, Thunderbird devrait afficher un bandeau de couleur verte au dessus du message.



IV - Commentaires

Merci d'adresser tous vos commentaires sur l'utilisation de ce guide à l'adresse : communication@aerodef.fr . Nous nous efforcerons de compléter ce document en fonction de vos demandes.