

# Postfix et DKIM

## OpenDKIM

### Installation

```
apt-get install opendkim opendkim-tools
```

### Configuration

Editer le fichier `/etc/opendkim.conf`

```
AutoRestart      Yes
AutoRestartRate  10/1h
UMask            002
Syslog           yes
SyslogSuccess    Yes
LogWhy           Yes

Canonicalization  relaxed/simple

ExternalIgnoreList refile:/etc/opendkim/TrustedHosts
InternalHosts     refile:/etc/opendkim/TrustedHosts
KeyTable          refile:/etc/opendkim/KeyTable
SigningTable      refile:/etc/opendkim/SigningTable

Mode             sv
PidFile          /var/run/opendkim/opendkim.pid
SignatureAlgorithm rsa-sha256

UserID           opendkim:opendkim

Socket           inet:17789@localhost
```

| Paramètre                       | Définition                                                                                                                                                   |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AutoRestart                     | Redémarrer automatiquement le service en cas d'erreur.                                                                                                       |
| AutoRestartRate                 | Le nombre de redémarrage maximum dans un temps donné. Par exemple, dix redémarrages par heure : 10/1h.                                                       |
| UMask                           | Accorder les permissions totales pour l'utilisateur défini par son userID, et accorder des permissions en lecture et exécution pour les autres utilisateurs. |
| Syslog / SyslogSuccess / LogWhy | Activer les journaux détaillés pour le service.                                                                                                              |
| Canonicalization                | La mise en forme canonique des messages de log.                                                                                                              |
| ExternalIgnoreList              | Les hôtes externes autorisés à envoyer des e-mails depuis ce serveur sans authentification.                                                                  |

| Paramètre          | Définition                                                                                                                          |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| InternalHosts      | Les hôtes internes pour lesquels les e-mails sortants doivent être signés.                                                          |
| KeyTable           | Assure la liaison des noms de clés avec les fichiers de clé.                                                                        |
| SigningTable       | La liste des signatures qui seront utilisées pour un message. Le choix se base sur l'adresse expéditrice.                           |
| Mode               | Le mode opératoire d'OpenDKIM. (s) signature et (v) vérification.                                                                   |
| PidFile            | Emplacement du fichier de pid contenant l'identifiant processus du service.                                                         |
| SignatureAlgorithm | L'algorithme de chiffrement choisi pour encoder les signatures.                                                                     |
| UserID             | L'utilisateur et son groupe qui exécutera le service OpenDKIM                                                                       |
| Socket             | Le port d'écoute sur lequel Postifx et OpenDKIM échangeront les messages. Pour écouter en local sur le port 17789: 17789@localhost. |

Editer le fichier /etc/default/openssl

```
SOCKET="inet:17789@localhost"
```

## Configuration des clés

Créer l'arborescence de clés

```
mkdir -p /etc/openssl/keys
```

Ajouter les hôtes et réseaux en liste blanche, fichier /etc/openssl/TrustedHosts:

```
127.0.0.1
localhost
172.80.0.0/21

*.ricozome.net
*.belhomme.eu
*.ricolan
```

Création du dictionnaire de clés /etc/openssl/KeyTable:

```
mail._domainkey.ricozome.net
ricozome.net:mail:/etc/openssl/keys/ricozome.net/mail.private
```

Création du dictionnaire de signature /etc/openssl/SigningTable:

```
*@ricozome.net mail._domainkey.ricozome.net
```

## Génération des clés

Création d'un répertoire par domaine:

```
mkdir -p /etc/openssl/keys/ricozome.net
```

Génération de clés:

```
cd /etc/openssl/keys/ricozome.net
openssl-genkey -s mail -d ricozome.net
chown openssl:openssl mail.private
```

## Création du record DNS DKIM

Visualisation de la clé publique:

```
cat /etc/openssl/keys/ricozome.net/mail.txt
mail._domainkey IN      TXT      ( "v=DKIM1; h=sha256; k=rsa; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAxllcurFBEj/Lsbm9xIZr5LakUnVri
kjUW1LXgwC5KRzpc/Q0pabCtgafsC4LjhA0ltz8eE6FfW6/iMl5D5mThoveF1HVna2lf3wVkuC7+
kk3EyJGcYTcZLHBiitlbmgh6fzVTI8nrsxouaCFyXJMTA0o3cEkXypecZp9D0qnHLY5GwwjFwZFJ
9AQPPlwEmuRtqXm9oN0mkNVaa"
"0gPEROC8pSpQyapGgSYTSld9GwsLL0fiVzybLVnK8ZhE0cYkW+xumyoe1DY5ix/xjFHTL8QMVRI
X2m3/H4RzHu+aFBYyVUjIWzqWQpIjVeCocVhJC+fPlONxCvT5pmYqmGZBT0QQIDAQAB" ) ; --
--- DKIM key mail for ricozome.net
```

Injection du record (format Bind) suivant:

```
mail._domainkey IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5N3lnvvrYgPCRSoqn+awTpE+iGY"
```

## Postfix

Edition de /etc/postfix/main.cf:

```
smtpd_protocol = 2
smtpd_default_action = accept

smtpd_milters = inet:localhost:17789
non_smtpd_milters = inet:localhost:17789
```

From:  
<https://www.ricozome.net/dokuwiki/> - Ricozome Wiki

Permanent link:  
[https://www.ricozome.net/dokuwiki/doku.php?id=pages\\_it:email](https://www.ricozome.net/dokuwiki/doku.php?id=pages_it:email)

Last update: **2020/02/04 10:02**

