

DKIM (BIND, Postfix/Exim)

Первый вариант.

Создаем каталог для размещения ключей:

```
mkdir /etc/opensslkim
```

Генерируем их:

```
opensslgenkey -D /etc/opensslkim/ --domain tst-am0.net.ua --  
selector relay
```

relay – название селектора (может быть любым напр. – *mail*)

Создалось два файла – **.private* – закрытый ключ (храним у себя), **.txt* – запись для DNS.

Создаем группу opensslkim:

```
pw useradd opensslkim -m -s /usr/sbin/nologin -w no
```

и меняем владельца:

```
chown :opensslkim /etc/opensslkim/*  
chmod g+r /etc/opensslkim/*
```

Второй вариант.

```
mkdir /usr/local/etc/exim/dkim
```

Делаем секретный ключ через openssl

```
root@server# openssl genrsa -out  
/usr/local/etc/exim/example.com.key 2048
```

На выходе имеем ключ вида:

```
-----BEGIN RSA PRIVATE KEY-----  
MIICXQIBAAKBgQDT1tSzyG2Zch4LTgGPbn/8H535Vd+friNn/gBsV7rFNVZdxa  
pD  
d0UzeATUTbAG/3Ux7vJxYd6i982IajVz0b2dsmkdDzctC4EdJsLcpCpyf3x21n  
YZ
```



```
c90DLm0FGpDQbXcRM+CTmX6H2jGkwJ4VcpqDwVZ"  
"RwIDAQAB" )
```

(В данном случае это синтаксис для DNS сервера на BIND, и другие DNS сервера могут не требовать знак “\” для экранирования “;”.)

Вместо **relay** можете использовать другой селектор, например, **dkim**, **server**, **public** и тд. Подобных записей Public key для DKIM может быть несколько.

Необходимо дождаться, когда обновится ваша DNS запись на других серверах. Это может занять несколько часов.

Проверять свою DKIM запись можно, например, с помощью сервиса [DNSWatch](#)

Добавляем ADSP запись

Создаем в DNS запись **_adsp._domainkey.example.com** типа TXT со значением **dkim=all**.

```
_adsp._domainkey.example.com. IN TXT "dkim=all"
```

Помимо **all** параметр **dkim** может иметь еще два значения – **unknown** и **discardable**.

- **unknown** – домен может подписывать некоторые или все письма.
- **all** – все письма с домена подписаны.
- **discardable** – все письма с домена подписаны. Кроме того, если письмо приходит без валидной подписи в связи с изменениями в пути, прохождением через путь без доступа к подписывающему ключу или по другим причинам, домен призывает адресата отклонить его.

Рестарт BIND.

Правим конфиг Exim

В файл */usr/local/etc/exim/configure* добавляем в начало:

```
## DKIM:
```

```
DKIM_DOMAIN = ${lc:${domain:$h_from:}} DKIM_FILE =  
/usr/local/etc/exim/${lc:${domain:$h_from:}}.key  
DKIM_PRIVATE_KEY = ${if exists{DKIM_FILE}{DKIM_FILE}{0}}
```

Эта конструкция позволит использовать разные Private key для разных доменов.

Подправляем транспорт **remote_smtp**:

```
remote_smtp:  
    driver          = smtp  
    dkim_canon      = relaxed  
    #dkim_strict    = yes  
    dkim_domain     = DKIM_DOMAIN  
    dkim_selector   = relay  
    dkim_private_key = DKIM_PRIVATE_KEY
```

Здесь **relay** — наш селектор, .

Сохраняем конфиг и перечитываем его:

```
root@server# service exim reload
```

Проверять DNS будем с помощью утилиты [dig](#), а также можно воспользоваться сервисом <http://www.dnswatch.info>

Проверка с помощью dig:

```
dig relay._domainkey.example.com TXT  
.....  
;; ANSWER SECTION:  
relay._domainkey.example.com. 3600 IN      TXT      "k=rsa\; "  
"p=MIIBIjA.....  
.....
```

С помощью сайта — в окошке выбираем тип записи *TXT* и вставляем
relay._domainkey.example.com

Postfix

Редактируем:

/etc/openssl.conf

И приводим его, например, к следующему виду:

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

Canonicalization      relaxed/simple

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

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

UserID               openssl:openssl

Socket               inet:12301@localhost
```

** все параметры можно оставить, как в данном примере, за исключением **Socket** – можно указать любой другой порт, вместо **12301**.*

Теперь создаем и заполняем файлы:

```
ee/etc/openssl/TrustedHosts
127.0.0.1
localhost
*.tst-amo.net.ua
```

```
ee /etc/openssl/KeyTable
relay._domainkey.tst-amo.net.ua          tst-
amo.net.ua:relay:/etc/openssl/relay.private
```

```
ee /etc/openssl/SigningTable
*@tst-amo.net.ua relay._domainkey.tst-amo.net.ua
```

Добавляем в автозагрузку и запускаем:

```
echo 'milteropendkim_enable="YES"' >> /etc/rc.conf
echo 'milteropendkim_uid="opendkim"' >> /etc/rc.conf
```

```
service milter-opendkim start
```

Вставляем в /usr/local/etc/postfix/main.cf

```
# DKIM
milter_protocol = 6
milter_default_action = accept
smtpd_milters = inet:localhost:12301
non_smtpd_milters = inet:localhost:12301
```

Перезапускаем и проверяем.

- <https://2keep.net/configure-dkim-exim-bind/>
- <https://habrahabr.ru/post/173605/>
- <https://www.dmosk.ru/instruktions.php?object=dkim-postfix>
- <https://www.fryaha.ru/freebsd-postfix-dkim/https://wiki.debian.org/ru/opendkim>
- <https://linode.com/docs/email/postfix/configure-spf-and-dkim-in-postfix-on-debian-8/>