DKIM (BIND, Postfix/Exim)

Первый вариант.

Создаем каталог для размещения ключей:

```
mkdir /etc/opendkim
```

Генерируем их:

```
opendkim-genkey -D /etc/opendkim/ --domain tst-amo.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 opendkim:

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

и меняем владельца:

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

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/gBsV7rFNVZdxapD
dOUzeATUTbAG/3Ux7vJxYd6i982IajVz0b2dsmkdDzctC4EdJsLcpCpyf3x21nYZ
```

```
oJO2GjaFW65MNj7dU7BXDerLTE+zTu/Q4vs4ZqCA39CtbmetjBS9l/NsMQIDAQ
AB
AoGBAM2ZyVFAatkQSBaivCLwlWknapSPgv4g7h5FSTXeI9i5frx+V1UnRDki+F
Tx
nbH9CErRZh8jZQj4x1Pp+T0SyRtb62ydJooPYIpNlTt71cgZNwH174uFt4HevK
mC
MJIhzaufEZYhamS4NQOR+4FakdZX2T8yzuvwDwkplJP2tO/tAkEA7RDltCTOSh
dd
sJYs0wjs1mDXUiSz0giFAYvMBvOelpyjJl9Pi1A0CNcD4WdvAl0Xo5aRMVrTXR
zf
-----END RSA PRIVATE KEY-----
```

Генерим публичный ключ на основе секретного

```
root@server# openssl rsa -in /usr/local/etc/exim/example.com.key -pubout
```

На выходе получим что-то вроде:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA3GNADCBiQKBgQDT1tSzyG1Zch4LTgGPbn/8H5
35
Vd+friNn/gBsV7rFNVZdxapDd0UzeATUTbAG/3Ux7vJxYd6i982IajVz0b2dsm
kd
DzctC4EdJsLcpCpyf3x21nYZoJO2GjaFW65MNj7dU7BXDerLTE+zTu/Q4vs4Zq
CA
-----END PUBLIC KEY-----
```

Создаем в DNS запись **relay._domainkey.example.com** типа TXT со значением:

```
mail._domainkey.example.com. IN TXT ( "k=rsa\; "
                                      "p=MIIBIjANBgkqhkiG9w0BAQE
FAAOCAQ8AMIIBCgKCAQEAs2WdcyOKgKVU2C/7CV77"
                                      "4mu/b+XVaVixtuASB0wAOjaPn
EcFzwI84hu6wmy8cpPJlVImnf1gD/y/pA08+viV"
                                      "PPP/6bHfEiJjxOSjDnhF2V1+G
lOrl6IYxNxOxXPLw88QpDPak+ZO0yLU58UxJP1K"
                                      "cPdCuftEMFHWd5vuiHquBNYtk
W6MxaGcoX4hK8eE9CdrKDH7EtuLkkJ4uj0Mw4R7"
                                      "kd6FexfyppDXFGGu8oDN+7IUf
CqnKDkUxqb5Dh4rDD24Tn6KdDY5eFgjw7OIUr8H"
                                      "Jbr9KNSE6lF3M5JLx9VX/ny3e
```

```
c9ODLm0FGpDQbXcRM+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/opendkim.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/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: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/opendkim/TrustedHosts
127.0.0.1
localhost
*.tst-amo.net.ua
```

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

```
ee /etc/opendkim/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/