DKIM (Domain Keys Identified Mail)

DKIM (Domain Keys Identified Mail) — технология подтверждения подлинности отправителя письма путём проверки цифровой подписи по открытому ключу в специальной DNS записи тип TXT домена отправителя.

http://dkim.org/

Можно использовать совместно с SPF (Sender Policy Framework)

Установка

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

Настройка

Для настройки нужно выполнить по порядку все следующие пункты:

1. Создание папки

   ```
   mkdir /etc/postfix/dkim/
   ```

2. Создание ключей

   ```
   opendkim-genkey -D /etc/postfix/dkim/ -d domain.ru -s mail
   ```

В результате создаются файлы:

```
mail.private
mail.txt
```

Для дальнейшего использования с несколькими доменами нужно переименовать файлы в соответствии с именем домена, пример для `domain.ru`:

```
mail.domain.ru.private
mail.domain.ru.txt
```

Внутренние хосты

Обязательно нужно внести в файл адрес (значение `inet_interfaces` из `/etc/postfix/postfix-o/main.cf`) выходного сервера, чтобы не возникала ошибка следующего вида: **`opendkim 10.0.0.1 not internal`**

/etc/postfix/dkim/InternalHosts

```
10.0.0.1
```

Список ключей

Формат: Имя_ключа Домен:Селектор:Имя_файла_ключа

/etc/postfix/dkim/KeyTable

```
mail._domainkey.domain.ru domain.ru:mail:/etc/postfix/dkim/mail.domain.ru.private
```

Список подписей

Формат: Домен Имя_ключа

/etc/postfix/dkim/SigningTable

```
domain.ru mail._domainkey.domain.ru
```

Завершение настройки

/etc/opendkim.conf

```
Syslog                  yes
UMask                   002
OversignHeaders         From
Canonicalization        relaxed/relaxed
AutoRestart             yes
DNSTimeout              5
SyslogSuccess           Yes
LogWhy                  Yes
Mode                    sv
UserID                  opendkim:opendkim
KeyTable                file:/etc/postfix/dkim/KeyTable
SigningTable            file:/etc/postfix/dkim/SigningTable
InternalHosts           file:/etc/postfix/dkim/InternalHosts
PidFile                 /var/run/opendkim/opendkim.pid
Socket                  inet:8891@localhost
```

Нужно задать параметры подключения:

/etc/default/opendkim

```
SOCKET="inet:8891@localhost"
```

 Обязательно нужно установить права на файлы:

dkim_rights.sh

```
#!/bin/bash

chgrp opendkim /etc/postfix/dkim/*
chmod g+r /etc/postfix/dkim/*
chmod 640 /etc/postfix/dkim/*.private
chown root /etc/postfix/dkim/*.private
chown root /etc/postfix/dkim/*.txt
```

Запуск:

```
service opendkim restart
```

Проверка:

```
netstat -tulpn|grep :8891
```

Postfix

В файл `main.cf` выходного сервера нужно добавить:

/etc/postfix/postfix-o/main.cf

```
milter_default_action = accept
milter_protocol = 2
smtpd_milters = inet:127.0.0.1:8891
non_smtpd_milters = inet:127.0.0.1:8891
```

Amavisd-new

Для того, чтобы Amavisd-new писал в заголовок поле `Authentication-Results` нужно:

/etc/amavis/conf.d/20-debian_defaults

```
$enable_dkim_verification = 1;
```

Roundcube

Для отображения статуса проверки DKIM в Roundcube нужно использовать расширение authres_status:

```
cd /tmp; wget https://github.com/pimlie/authres_status/archive/master.zip
```

DNS

Чтобы получатели могли проверить подлинность отправителя нужно создать специальную запись в зоне DNS нужного домена.

Имя записи	`mail._domainkey` Для домена третьего уровня `test` имя записи должно быть таким: `mail._domainkey.test`
Тип записи	`TXT`
Значение	Текст (внутри кавычек) из файла `/etc/postfix/dkim/mail.domain.ru.txt`

Почтовый клиент оправителя

Также важно, чтобы домен указанный в поле обратный адрес (записывается в поле `X-Sender`) совпадал с доменом, для которого сделан ключ, например: адрес должен быть `user@domain.ru` а не `user@sub1.domain.ru`

Тестирование

Для теста можно оправить тестовое письмо на любой из адресов:

```
check-auth@verifier.port25.com
```

```
check-auth2@verifier.port25.com
```

Также можно проверить домен на странице:DKIM Core

Ссылки

DomainKeys Identified Mail

https://wiki.debian.org/ru/opendkim

https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-dkim-with-postfix-on-debian-wheezy

https://www.port25.com/support/authentication-center/email-verification/

mindbox.fogbugz.com:Инструкция по настройке SPF и DKIM

Яндекс.Помощь: DKIM-подпись

domain name system - Setting up SPF and DKIM records of a subdomain - Server Fault

https://sysadminmosaic.ru/dkim/dkim

2020-08-01 15:20