OpenDKIM Plugin Documentation

Plugin providing OpenDKIM an implementation for i-MSCP.

Requirements

- i-MSCP versions >= 1.1.0
- Installed packages: opendkim, opendkim-tools

Existing milter configurations

This plugin will not check for an existing milter configuration in the Postfix main.cf file. If you need to add an extra milter, please ask in our forum!

1. Install needed Debian/Ubuntu packages if not already done

```
# aptitude update
# aptitude install opendkim opendkim-tools
```

2. Get the plugin from github

```
# cd /usr/local/src
# git clone git://github.com/i-MSCP/plugins.git
```

3. Create new Plugin archive

```
# cd plugins
# tar cvzf OpenDKIM.tar.gz OpenDKIM
```

4. Plugin upload and installation

- Login into the panel as admin and go to the plugin management interface
- Upload the OpenDKIM plugin archive
- Install the plugin

Update

1. Get the plugin from github

```
# cd /usr/local/src
# git clone git://github.com/i-MSCP/plugins.git
```

2. Create new Plugin archive

```
# cd plugins
# tar cvzf OpenDKIM.tar.gz OpenDKIM
```

3. Backup your current plugin config

```
# plugins/OpenDKIM/config.php
```

4. Plugin upload and update

- Login into the panel as admin and go to the plugin management interface
- Upload the OpenDKIM plugin archive
- Update the plugin list

Configuration

For the different configuration options please check the plugin config file.

```
# plugins/OpenDKIM/config.php
```

After you made your config changes, don't forget to update the plugin list.

- Login into the panel as admin and go to the plugin management interface
- Update the plugin list

Testing

Internal DKIM test

You could check on the command line if OpenDKIM is working for your domain:

```
# opendkim-testkey -d example.com -s mail -vvv
```

The result should look similar like this one. The 'key not secure' does not indicate an error. It is an expected consequence of not using DNSSSEC.

```
opendkim-testkey: checking key 'mail._domainkey.example.com'
opendkim-testkey: key not secure
opendkim-testkey: key OK
```

Query your DNS server and check the TXT DKIM record for your domain.

```
# dig -t txt mail._domainkey.example.com
```

External DKIM test

Open the link below and send a mail from the domain you activated OpenDKIM to the random mail address shown on that page.

```
http://www.brandonchecketts.com/emailtest.php
```

After you sent the mail, click on that page the 'View Results' button and verify the **DKIM Information:** section.

```
DKIM Information:

DKIM Signature


Message contains this DKIM Signature:
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=example.com;
    s=mail; t=1385558914;
    bh=fdkeB/A0FkbVP2k4J4pNPoeWH6vqBm9+b0C3OY87Cw8=;
    h=Date:From:To:Subject:From;
    b=ZtWi/eDZtQ0RDv60FCDf4c+G9gqhFH3r6RPCw9vr400auTH0PnkOwt2BuLNpv4Uh4
     wjBHhFnIqt+t/c9/DLCC8envKmnzco8BATgXl5I5HHLxDcGMFYlwHDgOLXcCKXOXA5
     15oFPlimBrwZXnq3XOJCwopZmUmZZhUyYT8pZO9k=


Signature Information:
v= Version:         1
a= Algorithm:       rsa-sha256
c= Method:          simple/simple
d= Domain:          example.com
s= Selector:        mail
q= Protocol:
bh=                 fdkeB/A0FkbVP2k4J4pNPoeWH6vqBm9+b0C3OY87Cw8=
h= Signed Headers:  Date:From:To:Subject:From
b= Data:
ZtWi/eDZtQ0RDv60FCDf4c+G9gqhFH3r6RPCw9vr400auTH0PnkOwt2BuLNpv4Uh4
     wjBHhFnIqt+t/c9/DLCC8envKmnzco8BATgXl5I5HHLxDcGMFYlwHDgOLXcCKXOXA5
     15oFPlimBrwZXnq3XOJCwopZmUmZZhUyYT8pZO9k=
Public Key DNS Lookup


Building DNS Query for mail._domainkey.example.com
Retrieved this publickey from DNS: v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDN+HbTA3/7KoENKhMr6qRO0cFeaDX1NSD5Xe
7zkGhkvOnajIrhycu0XyxzHLTTSbFLq9juJmUbPmP9OVj44o0p/NqoLQ9oWjfkcM+7nq+S4QYGoM
7h+SMcxjFm05mo0LdessYi/Sw5z6x87nMkLD/wQViDvctss4srrPTr/hqD+wIDAQAB
Validating Signature


result = pass
Details:
```

Authors

- Sascha Bay info@space2place.de
- Rene Schuster mail@reneschuster.de