By Andrew Colin Kissa

Published: 2008-01-30 17:18

Set Up Postfix DKIM With dkim-milterIntroduction

DKIM is an authentication framework which stores public-keys in DNS and digitally signs emails on a domain basis. It was created as a result of merging Yahoo's domainkeys and Cisco's Identified Internet mail specification. It is defined in RFC 4871.

We will be using the milter implementation of dkim **http://dkim-milter.sf.net** on CentOS 5.1

Installation

Install the rpm, ignore dependencies as csh is a dependency but it does not affect dkim-milter; it's only required for some sample scripts that are shipped with the rpm.

```
rpm http://www.c-corp.net/linux/centos/5/general/RPMS/i386/dkim-milter-2.2.1-1.i386.rpm --nodeps

mkdir /etc/dkim-milter

chown dkim-milt.dkim-milt /etc/dkim-milter

chmod 700 /etc/dkim-milter

chgrp postfix /var/run/dkim-milter

chmod 770 /var/run/dkim-milter
```

Generate The Keys

Download this **script** that you can use to easily generate the keys for signing the mail:

```
./dkim-genkey.sh -d <domainname>
```

Replace <domainname> with the domain name you will be signing mail for. This will create two files *default.txt* and *default.private*, *default.txt* is the line you need to add to your zone file - a sample is below:

```
default._domainkey IN TXT "v=DKIM1; g=*; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDG81CNNVOlWwfhENOZEnJKNlikTB3Dnb5kUC8/zvht/S8SQnx+YgZ/KG7KOus0By8cIDDvwn3ElVRVQ6Jhz/HcvPU5DXCAC5owLBf/gX5tvAnj
F1vSL8ZBetxquVHyJQpMFH3VW37m/mxPTGmDL+zJVW+CKpUcI8BJD03iW2l1CwIDAQAB"
; ----- DKIM default for topdog-software.com
```

default.private contains your private key. Move this file into */etc/dkim-milter* and rename it *<domainname>_default.key.pem*:

```
mv default.private /etc/dkim-milter/<domainname>_default.key.pem
```

Edit the file */etc/sysconfig/dkim-milter* and set the variables:

```
USER="dkim-milt"
PORT=local:/var/run/dkim-milter/dkim.sock
SIGNING_DOMAIN="<domainname>"
SELECTOR_NAME="default"
KEYFILE="/etc/dkim-milter/${SIGNING_DOMAIN}_${SELECTOR_NAME}.key.pem"
SIGNER=yes
VERIFIER=yes
```

```
CANON=simple
SIGALG=rsa-sha1
REJECTION="bad=r,dns=t,int=t,no=a,miss=r"
EXTRA_ARGS="-h -l -D"
```

Init Script Fix

Install my modified init script as the one that is supplied with the rpm has a bug.

```
wget http://www.topdog-software.com/files/dkim-milter -O /etc/init.d/dkim-milter

chkconfig --level 345 dkim-milter on

service dkim-milter start
```

Configure Postfix

Add this to the postfix configuration file `/etc/postfix/main.cf`:

```
smtpd_milters = unix:/var/run/dkim-milter/dkim.sock
non_smtpd_milters = unix:/var/run/dkim-milter/dkim.sock
```

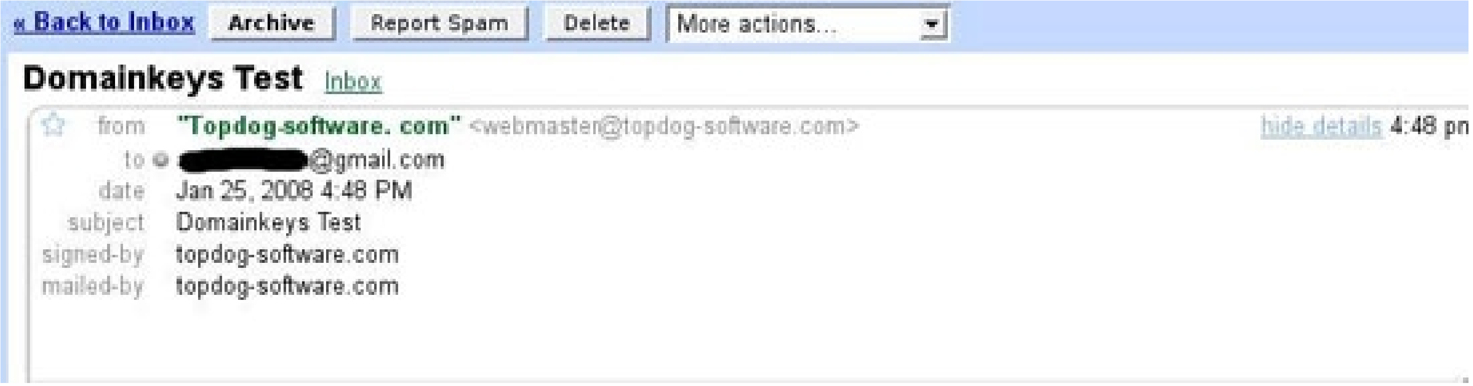
Append to the existing milters if you have other milters already configured.

Restart Postfix:

```
service postfix restart
```

Testing

Send a message to autorespond+dkim@dk.elandsys.com; the system will return a response to let you know if DKIM is working. Examine the headers of mails from domains like gmail to see if your system is checking the DKIM signatures of inbound mail.



Domainkeys Test

from "Topdog-software. com" <webmaster@topdog-software.com> 4:48 pn
to [redacted]@gmail.com
date Jan 25, 2008 4:48 PM
subject Domainkeys Test
signed-by topdog-software.com
mailed-by topdog-software.com

DKIM mail in Gmail