DKIM - DomainKeys Identified Mail


Nakon što smo u borbi protiv spama posegnuli za SPF-om [1] (***Sender Policy Framework***), sada ćemo pogledati kako radi DKIM - ***DomainKeys Identified Mail.*** Ova se dva sustava lijepo nadopunjuju i ne miješaju se jedan drugome u posao. Pojednostavljeno, zapis SPF govori "*da, ovaj mail potiče s jednog od autoriziranih servera za slanje maila s naše domene*". DKIM ide korak dalje i kriptografski potpisuje poruku, a time govori "*ova poruka potječe s naše domene i nije promijenjena u transportu*".
DKIM je nastao 2005. godine kao amalgam između specifikacije ***DomainKeys*** (razvio Yahoo) i IIM - ***Identified Internet Mail*** (razvio Cisco). DKIM omogućava da se pojedinoj poruci "pridruži" domena, čime je omogućena provjera autentičnosti poruke putem standardnih kriptografskih metoda (javnih i privatnih ključeva). Javni ključ se distribuira preko DNS-a (slično kao i kod SPF-a).

Ustanova (odnosno "*signer*") svojim ključem garantira da mail potječe s te ustanove, ali ne preuzima odgovornost za sadržaj maila, pošiljatelja ili primatelja. Primatelj ("*verifier*") može provjeriti autentičnost poruke pogledavši javni ključ u DNS zapisu. DKIM kriptografski štiti sadržaj maila i neka zaglavlja, što mu daje sposobnost da preživi routing preko nekoliko mail servera. Iz toga proizlazi da DKIM ne može baš u svim situacijama u potpunosti garantirati integritet poruke od pošiljatelja do primatelja, ali zapravo to mu ni nije glavna namjena. Ako baš želite biti sigurni da nitko nije modificirao vašu poruku ili barem zaglavlja, koristite neki kriptografski program.

Više možete naći na stranicama http://www.dkim.org/ [2] ili na Wikipediji.

Kako podesiti DKIM na standardnim CARNetovim poslužiteljima s Debianom? Prije svega, treba instalirati neke pakete:

```
# apt-get install opendkim
...
The following extra packages will be installed:
  libev3 libldns1 libmilter1.0.1 libopendkim1 libunbound2
```

(postoji i paket dkim-filter, odnosno dkim-milter, ali on se više neće održavati)

Paket opendkim će povući i libmilter1.0.1 (da, to je onaj mail+filter = milter kojeg smo davno koristili kod sendmaila!). Sljedeći korak je generiranje DKIM ključa.

```
# opendkim-genkey -t -s mail -d domena.hr
```

Opcija -t omogućava testni mod, koji možete koristiti dok se sve ne uskladi. Navodno većina drugih servera tako i radi, u testnom modu, pa je na udaljenim serverima odluka hoće li poštivati DKIM ili neće.

```
# ls -l mail*
-rw------- 1 root root 891 Feb 26 14:11 mail.private
-rw------- 1 root root 300 Feb 26 14:11 mail.txt
```

Dobili smo dvije datoteke. Jedna je privatni ključ (mail.private), kojeg ćemo prebaciti u direktorij /etc/mail/, a druga je javni ključ kojeg ćemo staviti u DNS.

```
# cp mail.private /etc/mail/dkim.key
# catmail.txt
 mail._domainkey IN TXT "v=DKIM1; g=*; k=rsa; t=y;
 p=MIGfMA0GCOlkfds3DQEB67UAA5jNADCkOQKBWWCvLDPMAQR+FCve4lWVecx+R2D2/C3PO...."
 ; ----- DKIM mail for domena.hr
```

Kao i kod SPF-a, ovaj zapis treba dodati u zonsku datoteku vaše domene. Nećemo više ponavljati kako se to radi, da treba povećati Serial itd. Samo na kraju ne zaboravite restartati Bind:

```
# rndc reload
server reload successful
```

U konfiguracijskoj datoteci **/etc/opendkim.conf** se već nalaze neke zakomentirane vrijednosti. Samo nekolicinu treba promijeniti odnosno dodati, iako opcija ima još:

```
Syslog                  yes
#LogWhy                  yes
UMask                   002
Domain                  domena.hr
KeyFile                 /etc/mail/dkim.key
Selector                mail
Canonicalization        relaxed/simple
```

Zatim trebate otvoriti datoteku **/etc/default/opendkim** i odkomentirati redak:

```
SOCKET="inet:12345@localhost" # listen on loopback on port 12345
```

DKIM server će nakon ovoga slušati na portu 12345, i to na *loopback* adresi, što znači da se na taj port neće moći spajati nitko s Interneta, što je dobro sa sigurnosnog stanovišta.

Pokrenimo DKIM filter:

```
# /etc/init.d/opendkim start
# pgrep opendkim
14294
```

Daemon se startao, a ako nije pogledajte u logovima zašto. Možete dodati i opciju "**LogWhy yes**" u opendkim.conf kako bi vidjeli više informacija u logovima.

Sada trebamo podesiti Postfix, odnosno milter. Na kraj datoteke **/etc/postfix/main.cf** dodajte sljedeće (smiješno da nakon ovoliko godina rada uopće spominjemo gdje se nalazi koja konfiguracijska datoteka) :

```
milter_default_action = accept
# Milter protokol je "6" za Postfix >= 2.6, ina?e je "2"
milter_protocol = 6
smtpd_milters = inet:localhost:12345
non_smtpd_milters = inet:localhost:12345
```

Restartajte Postfix i pratite logove.

Ukoliko je sve u redu dobit ćete u zaglavlju mail jedno novo zaglavlje:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=domena.hr; s=mail;
    t=1361353867; bh=vBY0FVCZ0hSxDP+kMyke+SVdBiszOUn/U+n4HC73vkw=;
    h=Date:From:To:Subject:Message-ID:MIME-Version:Content-Type;
    b=5D9kliifgXS6fOSXqbnunr0xOLIKJnjd71n7DwetWtbFHg7a7u/aSlWlE2lS0lNye
     ltkNtI69Xs+pOplvr5%$/LKFIFN7YKO5rywC/zdJBhA0KXVdM+PKXmLT1Aw6yDdK8k
     t4FlCMbdnkjKJpGw/HLqtlFhvx7A99qntelUWgLs=
```

Ispravnost ovog novog zaglavlja možete rovjeriti na adresi http://dkimcore.org/tools/ [3]. To vam svakako preporučujemo. U svakom slučaju greške su moguće. Jedna od češćih je ovakva poruka kod startanja:

```
# /etc/init.d/opendkim start
Starting OpenDKIM: opendkim: /etc/opendkim.conf: at least one selector and
key required for signing mode
opendkim.
```

Ova poruka znači u konfiguracijskoj datoteci niste odredili lokaciju ključa (**KeyFile**) ili tzv. selektor (**Selector**), ili oboje.

Feb 27 23:59:56 server dkim-filter[411]: 81BA7E778: no signature data

Gornju poruku ne bi trebali dobiti, jer ona znači da se konfigurirana domena ne poklapa s onom koju zaista koristite u mailovima. Ukoliko mislite da je s vašim sustavom sve u redu, možete probati staviti *wildcard* (*) umjesto naziva domene:

```
Domain                  *
```

Zdravko Rašić

sri, 2013-02-27 22:54 - Zdravko Rašić**Kuharice:** Linux [4]
Kategorije: Software [5]
Servisi [6]
Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

story_tag: DKIM [7]

Source URL: https://sysportal.carnet.hr/node/1217

Links
[1] https://sysportal.carnet.hr/node/1215
[2] http://www.dkim.org/
[3] http://dkimcore.org/tools/
[4] https://sysportal.carnet.hr/taxonomy/term/17
[5] https://sysportal.carnet.hr/taxonomy/term/25
[6] https://sysportal.carnet.hr/taxonomy/term/28
[7] https://sysportal.carnet.hr/taxonomy/term/149