DKIM - DomainKeys Identified Mail

Zdravko Rašić | 27 veljače, 2013

Nakon što smo u borbi protiv spama posegnuli za SPF-om (***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/ ili na Wikipediji.

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

(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.

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.

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.

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.

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:

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

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

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:

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) :

Restartajte Postfix i pratite logove.

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

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

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: