HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA - CARNet

CDA0015

POSLUŽITELJ JAVNIH *PGP* KLJUČEVA (*PKS*) U CARNet-U

Ur.broj: 1-98-5-018 **Kategorija: PREPORUKA** **Trajanje: do opoziva**

Datum nastanka: 11.06.1998. **Verzija: 1.0 (11.06.98.)**

URL: ftp://ftp.carnet.hr/pub/CARNet/docs/advisories/CDA0015.pdf

1. Uvod

PGP program autora *Phila Zimmermanna* jedan je od danas najpopularnijih i najraširenijih programa korištenih za kriptografsku zaštitu podataka. Sam program koristi asimetričan kriptografski algoritam, što će reći da korisnici rabe dva tipa ključeva: **javni** i **tajni**.

Da bi kriptografski zaštitili određeni sadržaj tako da ga samo određene osobe mogu pročitati dovoljno je posjedovati **javne ključeve** tih osoba. Zaštićeni sadržaj mogu pročitati **jedino** osobe čiji su javni ključevi korišteni pri kriptiranju i to putem vlastitih tajnih ključeva.

Tajni ključ je tajna informacija koju korisnik zadržava za sebe dok je javni ključ javna informacija koju korisnik objavljuje na neki način (primjerice: *finger* informacija, osobna *WWW* stranica, posjetnica i sl.). Način objavljivanja javnih ključeva koji se uspio nametnuti kao *de-facto* standard je putem specijaliziranog **poslužitelja javnih PGP ključeva** (engl. ***P**GP **K**ey**S**erver, **PKS***).

Više informacija o načinu rada PGP programa i algoritmima kriptiranja možete pronaći na sljedećim URL-adresama:

- `http://www.pgp.com` (*En.*, informacije o američkoj verziji *PGP* programa)
- `http://www.pgpi.com` (*En.*, informacije o internacionalnoj verziji *PGP* programa)

2. Što je PKS?

PKS odnosno *poslužitelj javnih PGP ključeva* je razvijen na *MIT*-u a autor mu je *Marc Horowitz*. Zamišljen je kao sustav za distribuciju i pohranjivanje javnih *PGP* ključeva u digitalnom obliku. Iako poslužitelj može biti potpuno centralizirane naravi i neovisan u radu to nije pravilo. Naime *PKS* poslužitelji se obično povezuju putem Interneta i na taj način međusobno razmjenjuju promjene u bazama podataka odnosno nove ključeve. Nije dakle potrebno svoj javni ključ dostavljati svim poznatim PKS poslužiteljima već samo najbližem u lancu.

PKS se može koristiti kako sa starijom verzijom *PGP* ključeva (tzv. RSA ključevi), tako i s novijom verzijom *PGP* ključeva (tzv. D/H ključevi). Isto tako, novije verzije *PGP* programa imaju već ugrađenu podršku za pretraživanje i dohvaćanje ključeva putem *PKS* poslužitelja ukoliko traženi javni ključ ne posjeduju lokalno.

PGP program barata sa dvije ***ID*** identifikacijske oznake ključa: simboličkom ***UserID*** i numeričkom ***KeyID*** oznakom. Upravo su te oznake elementi po kojima se obavlja pretraživanje baze *PKS* poslužitelja. Ukoliko koristimo *KeyID* identifikacijsku vrijednost koja je predstavljena nizom od *8* heksadecimalnih znamenaka moramo ispred vrijednosti upisati "`0x`".

Sam PKS poslužitelj ne koristi jake kriptografske algoritme niti je njime moguće kreirati nove ključeve tako da ne spada pod striktne američke zakone o izvozu jake kriptografije i tzv. *ITAR* pravila. Glavna zadaća koju poslužitelj obavlja, prikupljanje i distribucija javnih *PGP* ključeva, također nije podložna izvoznim ograničenjima SAD-a, zemlje odakle originalna verzija poslužitelja potječe.

3. CARNetov PKS *poslužitelj*

CARNetov poslužitelj javnih PGP ključeva instaliran je na računalu **`ds.carnet.hr`** i dio je mreže sličnih poslužitelja unutar lanca **`keys.pgp.net`** pod adresom **`keys.hr.pgp.net`**.

Svim korisnicima CARNeta kao i svim ostalim korisnicima Interneta u Hrvatskoj preporučamo uporabu CARNetovog *PKS* poslužitelja za objavu javnog *PGP* ključa.

Poslužitelju se može pristupiti:

a) slanjem elektroničke pošte na adresu:

`pgp-public-keys@carnet.hr`

b) putem WWW sučelja na adresi:

`http://ds.carnet.hr/pgp-public-keys/`

Iako se u dosadašnjoj praksi PKS uglavnom rabio putem e-pošte, **preporučamo** korisnicima da CARNetov PKS rabe **putem WWW sučelja**.

Upute za rad i dodatne informacije u svezi *PKS* poslužitelja nalaze se na adresi:

`http://ds.carnet.hr/pgp-public-keys/upute.html`

Kontakt adresa za sva pitanja i prijedloge vezane uz CARNetov PKS je:

`pgpadmin@carnet.hr`