HOWTO za srečanje z podpisovanjem GPG/PGP ključev

Avtor: *V. Alex Brennen* (*vab@cryptnet.net*) Prevod:*Boštjan Müller* (*neonatus@neonatus.net*) v1.0.4, 21. junij 2001, prevod: 22. december 2001

Ta dokument opisuje postopek in metode za organizacijo ter udeležbo na srečanju s podpisovanjem PGP/GPG ključev z uporabo GPG PGP implementacije, GnuPG. Ponudi nam razlago postopka za srečanje s podpisovanjem, odgovore pogosto zastavljenih vprašanj ter razloži kako proizvesti svoje in podpisovati ključe drugih ljudi.

Kazalo

1 Pregled srečanja

1.1 Kaj natanko je srečanje s podpisovanjem ključev?

Srečanje s podpisovanjem GPG/PGP ključev (GPG/PGP Keysigning Party) je shod GPG/PGP uporabnikov z namenom srečanja z drugimi uporabniki GPG/PGP-ja ter podpisovanjem ključev. To v veliki meri pripomore k razširjanju mreže zaupanja (web of trust), včasih pa služi kot forum za diskusijo o močni enkripciji, političnih, ter socialnih spornih točkah na temo močne enkripcije, pravicah posameznikov, neodvisnosti posameznika ter celo implementaciji enkripcijske tehnologije ali celo bodoče delo na prostem programju za enkripcijo.

1.2 Kaj je podpisovanje ključev?

Podpisovanje ključev je digitalni podpis javnega ključa. Digitalno lahko podpišete svoj lastni ključ, ali pa javni ključ, ki pripada nekomu drugemu. Podpisovanje ključev je potrebno, da se preveri, da določen javni ključ res pripada osebi, ki se izdaja kot lastnik ključa. Na nek način podpisi overjajo javne ključe. Na ta način podpisovanje ključev širi mrežo zaupanja.

1.3 Kaj je mreža zaupanja (web of trust)?

Mreža zaupanja je izraz, ki se uporablja za opis odnosa med skupinami ključev. Podpis ključa je kot povezava ali nit če temu tako rečemo v mreži zaupanja. Te povezave so imenovane *Pot Zaupanja (Trust Path)*. Poti zaupanja so lahko obojstranske ali le enosmerne. Ideana mreža zaupanja je takšna v kateri je vsak obojestransko povezan z vsemi ostalimi. Efektivno vsk zaupa, da vsak ključ dejansko pripada lastniku. Mrežo zaupanja si lahko predstavljate kot vsoto vseh teh poti zaupanja, ali povezav med vsemi lastniki ključev. Kot grafičen primer si lahko ogledate primer *grafa mreže zaupanja* v katero spada avtor tega HOWTO-ja.

1.4 Mi lahko daste primer uporabe podpisa z ključi?

Kot primer, recimo, da Alice in Bob generirata ključe z GPG-jem ter priredita PGP srečanje s podpisovanjem ključev. Na srečanju Alice in Bob drug drugemu overita informacije o ključih in kasneje drug drugemu podpišeta ključe. GPG že privzeto avtomatsko podpiše javni ključ vsakega generiranega para z pripadajočim privatnim ključem. Tako imata sedaj Alice in Bob vsaj dva veljavna podpisa, ki potrjujeta, da jima ključa res pripadata. Ključ, ki pripada Alice je podpisan od Alice same, ter Bob-a, Bob-ov ključ, pa vsebuje njegov lasten podpis ter podpis Alice. Če v prihodnosti Bob in Alice srečata Cathy. Cathy generira par ključev, ter in pove Alice in Bob-u da jima bo poslala svoj ključ. Alice Cathy ni všeč in noče, da bi Bob komuniciral z njo preko enkriptiranih podatkov. Obe Alice in Cathy generirata PGP ključe, kateri naj bi oboji pripadali Cathy. Obe pošljeta ključ Bob-u. Oba ključa imata le en podpis, podpis pripadajočega privatnega ključa. Bob ne ve kateri ključ dejansko pripada Cathy. Cathy izve, da je Bob dobil dva ključa in sumi Alice. Cathy, sedaj jezna, želi pridobiti informacije, katere bi lahko uporabila proti Alice. Če pa to hoče storiti mora komprimirati enkriptirano komunikacijo med Alice in Bob-om. Da pa bi to dosegla, se Cathy odloči ponarediti email od Alice Bob-u v katerem mu sporoča, da je generirala nov set ključev. Ponarajenem e-mailu Cathly doda "novi"javni ključ (ki je v bistvu ponarejen ključ, katerega je generirala Cathy). Vendar Bob, ki ima sedaj dva ključa od Alice, enega od teh je podpisalo več ljudi (on in Alice), kar potrdi, da ta ključ pripada Alice, medtem, ko ima drugi ključ (ključ, katerega je ponaredila Cathy samo en podpis - lasten podpis).

Zgornji primer je zelo poenostavljen in stvari so lahko dosti bolj zakomplicirane kot to. Za več informacij in detajlne opise si lahko preberete PGP FAQ-a ali dobre knjige o PKI. Zgornji primer jasno razloži osnove podpisovanja ključev in vrednost le-tega. Cathy ni bila zmožna zamenjati ključa zaradi povezav mreže zaupanja med Bob-om in Alice.

Kakorkoli, podpisi in mreže zaupanja ne jamčijo za verodostojne ključe. Na primer, ko sta Bob in Alice prvič srečala Cathy, recimo, da je Cathy-in prijatelj Donald bil z Cathy. Donald bi lahko generiral ponarejene pare ključev za Alice in Bob-a, ju podpisal z svojim ključem ter nato še vsakega z vsakim, kar bi imelo za posledico ključe z tremi podpisi na vsakem ključu, katere bi nato poslal Cathy Cathy bi tako imela serije ponarejenih ključev in podpisov. Kako bi njej pomagalo podpisovanje ključev, da bi se lahko obranila takšnega napada? Recimo, da so vsi ljudje vpleteni ključe izmenjevali preko strežnikov s ključi (keyservers). Če bi Cathy iskala Bob-ov in Alice-in ključ preko strežnika s ključi bi našla dva primera ključev tako za Alice kot za Bob-a. Če pa bi Alice in Bob dobila dvajset podpisov na srečanju z podpisovanjem ključev, je očitno, da Cathy lahko bolje zaupa ključu, podpisanemo dvajsetkrat kot ključu podpisanemu trikrat. Cathy bi lahko dobila nekaj informacij o ključih tudi iz obstoja dodatnih javnih ključev - pobližje si lahko ogleda čas generiranja in datume ter mrežo zaupanja teh ključev. Dvajset ključev, z podpisov z srečanja z podpisovanjem bi morali biti podpisani dvajset ali večkrat, ter bi morali imeti različne čase generiranja, najverjetneje bi bili vsi ključi, ki so podpisali Alice-in in Bob-ov ključ podpisani tudi z drugimi ključi. To pa se nebi zgodilo, če bi Donald heneriral dvajset ponarejenih parov ključev, ter sam ustvaril ponarejeno mrežo zaupanja.

1.5 Zakaj bi hoteli prirejati lastna srečanja s podpisovanjem ključev?

Obstajajo trije osnovni razlogi, zakaj bi priredili čim več srečanj s podpisovanjem ključev.

Prvič ter morda najpomembneje, priredite čim več srečan s podpisovanjem ključev, da razširite mrežo zaupanja. Globje in bolj povezana kot bo, težje jo je prevarati.

Drugič, srečanja s podpisovanjem ključev omogočajo vključitev drugih v "varnostno kulturo"in jih spodbujajo k razumevanju PGP-ja in povezane tehnologije za močno enkripcijo. Da bi pridobili prednosti močne enkripcije jo morajo ljudje uporabljati in to pravilno.

Končno, srečanja s podpisovanjem ključev pripomorejo k izgradnji skupnosti. Pripomorejo "tekijem"(techies) da se družijo, spoznajo en drugega, mrežo, ter diskutirajo o pomembnih temah kot so pravice posameznikov, pravice enkripcije, pravila interneta. Diskusija je pomembna, ker je ne le prvi korak, temveč korak pred akcijo. V času avtorjevega pisanja tega dokumenta na svetu ni ravno mnogo mrež zaupanja. Če delate na tem, da bi zgradili mrežo zaupanja v vašem okolišu, je zelo verjetno, da bodo prvi udeleženci v tej mreži voditelji ter tisti, ki bodo ustvarjali pravila internetne skupnosti v vašem okolišu. To so posamezniki, ki lahko izberejo da zgradijo močno varno kriptografijo in protokole v lokalno infrastrukturo, če si tega želijo. Integracija takšne tehnologije in protokolov bi povzročile, da bi problemi, kot je FBI-jev carnivore sistem neizvedljiv in zatorej dvomljiv.

2 Organizacija srečanja

2.1 Vloga koordinatorja

Srečanja s podpisovanjem ni zelo težko organizirati ali koordinirati. Kakorkoli, poleg rednih nalog povabljanja ljudi, izbire lokacije ter določitve časa, ima koordinator še naloge specifične za srečanje s podpisovanjem. Te navadno vključujejo pripravljanje spiska ključev za vsakega udeleženca, ter določitev zgradbe srečanja.

2.2 Kako naj bi bilo srečanje strukturirano?

Obstajata dva osnovna načina, na katera lahko izgradimo srečanje s podpisovanjem ključev – centraliziran način ali decentraliziran način. Najboljši pristop k srečanja se določi glede na količino ljudi, ki bodo na srečanju prisostvovali, ter ozračja lokacije, kjer se bo srečanje odvijalo. Osnovne zahteve srečanja so da so udeleženci zmožni overiti ključe drug drugemu ter identitete drug drugemu. Če so te osnovne zahteve izvršene lahko koordinator uporabi variacije teh dveh tipov.

Centralizirano srečanje bi bilo bolj organizirane oblike, kar bi bolje delovalo z manjšimi števili ljudi. Udeleženci pošljejo podatke o svojih ključih koordinatorju, ki te podatke shrani v spisek. Vsak udeleženec, potem ko prispe na srečanje dobi en izvod tega spiska. Vsakega udeleženca bi potem poklical koordinator. Udeleženec bi takrat preveril, če se njegov fingerprint ujema z fingerprintom ključa na spisku, katerega jim je dal koordinator. Če je udeleženec prepričan, da je fingerprint pravilen, bi na glas prebral svoj fingerprint, tako, da bi še ostali udeleženci videli, da imajo na listu pravi fingerprint. Če se fingerprint ujema, ga odkljukajo na svojem listu. To je nujno, da se preveri, da koordinator ni naredil napake pri pripravljanju spiska ali da jim ni podtaknil spisk z ponarejenimi podatki. Po tem, ko so vsi odkljukali ključ, koordinator pokliče naslednjega udeleženca, ter tako dalje. Po tem, ko so vsi ključi obkljukani, se udeleženci ter koordinator postavijo v vrsto, pred seboj pa držijo list z svojim ID-jem. Oseba na začetku vrste se sprehodi do konca vrste in preveri ID vseh oseb v vrsti. Če je ID pravilen in se ujema s tem na listu, ter že ima prvo kljukico si odkljuka poleg ključa še drugo kljukico. Ko ima ključ enkrat dve kljukici se ga lahko podpiše.

Decentralizirano srečanje bi temeljilo na principu da vsak dela zase. Udeleženci naj bi se pomečali neformalno, ter poiskali ostale udeležence katerih ključev še niso podpisali. Po srečanju preverijo ključe na svojih spiskih ter edendrugemu overijo ID-je. Decentralizirana srečanja omogočajo vključitev dosti večjega števila ljudi, vendar imajo tudi slabo lastnost, da udeleženci lahko spregledajo koga in mu ne podpišejo ključa. Na takšnem srečanju je pomembno, da koordinator vzpodbuja vse, da se prepričajo, da so overili ID-je ostalih. Spisek ključev ter fingerprintov ni nujen za takšno srečanje, je pa priporočljiv.

Centralizirana srečanja so odlična za podpisovanja na konferencah med kosilom, neformalnih tihih srečanjih pri nekom doma ali vrestavraciji, itd. Decentralizirana srečanja so dosti bolj praktična za srečanja, katerih se bo udeležilo večje število ljudi, in se odvijajo v baru ali kakem drugem hrupnem okolju, ali zabavah katerih se udeležujejo neotesani ter težko kontrolirajoči geek-i.

2.3 Naznanitev srečanja

Večje kot je srečanje tem bolje. Srečanje lahko naznanite na lokalnem LUG poštnem spisku, ostalih spiskih povezanih z računalništvom v vaši okolici, lahko celo daste oglas v časopis ali izdate bilten za tisk.

Če ravno začenjate graditi mrežo zaupanja v vašem okolišu, je navadno pametno združiti čim več aktivnih PGP uporabnikov, da vam pri tem pomagajo, ker so oni navadno tisti, ki bodo v prihodnosti organizirali takšna srečanja. Dobri načini iskanja takšnih ljudi so pogovori z ostalimi, ki pošiljajo PGP podpisana sporočila na poštne spiske, ali z iskanjem ključev z e-mail naslovi specifičnimi za vaš okoliš na strežnikih s ključi. Naprimer e-mail naslovi, ki se končajo z domenami univerz ali večjih podjetih lociranih v vašem okolišu pogosto privedejo do velikega števila zainteresiranih oseb.

Tu je nekaj primerov naznanil:

- *Spletna stran naznanitve srečanja s podpisovanjem PGP ključev*
- *E-mail naznanitve srečanja s podpisovanjem PGP ključev*
- *Bilten za tisk naznanitve srečanja s podpisovanjem PGP ključev.*

2.4 Ustvarjanje spiska ključev

Če boste uporabili strukturo za srečanje, pri kateri udeleženci potrebujejo spisek ključev vseh prisostujočih, mora koordinator takšen spisek tudi ustvariti. Spisek naj bi bil sestavljen na način podoben temu:

Key ID	Key Owner	Key Fingerprint	Key Siz
992A4B3F	V.Alex Brennen <vab@cryptnet.net>	0EC8 B0E3 052D FC4C 208F 76EB FA92 0973 992A 4B3F	1024

Avtor je napisal perl skripto, ki generira HTML dokument v zgornjem stilu iz gpg keyring-a, jaz sem jo malce spremenil, tako, da deluje tudi z novejšimi verzijami gpg-ja. *Perl* skripta ki generira spisek ključev je dosegljiva pod pogoji GNU General Public License (GPL).

Kopije spiska bi se nato natisnilo za vse udeležence srečanja s podpisovanjem. Koordinator lahko natisne spisek sam, ali pa ga razpošlje udeležencem preko e-mail-a ali pa ga objavi na spletni strani, ter ga nato udeleženci natisnejo sami.

2.5 Grafična izrisava mreže zaupanja (web of trust)

Nič ne vzpodbudi zanimanja ljudi kot pisane slike. Zatorej, izrisovanje mreže zaupanja kot ste jo izgradili v vašem okolišu lahko pripomore k motivaciji ljudi, da sodelujejo, kot tudi to, da vsem jasno prikaže kaj ste dosegli v procesu.

Enostavno lahko izdelate graf vseh ključev in podpisov vaše mreže zaupanja z pretvorbo teh informacij v dot datoteko, katero lahko podate programu za izrisovanje grafov kot sta dot ali neato. Perl skript, ki pretvori keyring v datoteko dot formata je napisal Darxus in je ravno tako dosegljiva pod pogoji GPL. Da lahko narišete graf mreže zaupanja boste morali na svoj disk shraniti Darxus-ov *sig2dot.pl* skript ter AT&T Researchh-ov *graphviz* paket. Morda ne boste mogli generirati grafa mreže zaupanja za več kot nekaj sto vozlišč ker je za takšno operacijo potrebno kar nekaj spomina.

Navodila za risanje grafa mreže zaupanja v gpg keyring-u so vključena v sig2dot.pl skriptu, ali pa jih lahko najdete na Debian-ovi strani o risanju grafof keyringov. Zopet tule je *povezava na graf mreže zaupanja* ki je bil narejen z sig2dot.pl skriptom ter neato programom za grafe. Več informacij je dosegljivih preko *Debian keyring graphing page (en)*.

3 Udeležba na srečanju

3.1 Povzetek nalog udeleženca srečanja

1. Generati par ključev
2. Pošljite javni ključ na določen strežnik s ključi (ali koordinatorju)
3. Pošljite podatke o javnem ključu koordinatorju
4. Prikažite se na srečanju
5. Preverite podatke o vaših ključih na srečanju
6. Preverite podatke o ključih vseh ostalih na srečanju
7. Podpišite vse preverjene ključe
8. Pošljite vse podpisane ključe nazaj na strežnik s ključi (ali lastniku ključa)

3.2 Kaj naj udeleženci prinesejo na srečanje?

1. Njih same - virtualno ne morete prisostvovati
2. Dve vrsti dokumenta s sliko - vozniško dovoljenje in osebna izkaznica sta dovolj
3. Key ID, Key Type, Hex Fingerprint and Key Size informacije o svojem ključu na listu
4. Pisalo

3.3 Česa naj udeleženci Nebi Prinesli na srečanje?

1. Računalnika

3.4 Zakaj naj nebi prinesli računalnika na srečanje?

Računalnika naj nebi prinesli na srečanje ker lahko binarne zamenjave ali modifilacije sistema enostavno komprimirajo PGP sisteme.

Če naj bi nekdo prinesel prenosnik katerega naj bi vsi uporabljali za podpisovanje ključev na srečanju, nebi nihče dejansko vedel, ali je na računalniku tekel program, ki lovi vtipkane znake, modificirano verzijo GPG-ja, modificirano verzijo Linux jedra ali posebno oblikovano tipkovnico, katerikoli od teh načinov bi se lahko uporabil, da bi pridobili privatne ključe tistih, ki so uporabljali računalnik.

Uporaba računalnika na srečanu bi vas ravno tako naredila ranljive za branje preko ramena, ali bolj kompleksne napade kot je injekcija virusov, ki modificirajo gpg program, da bi izdajali podatke o privatnih ključih.

3.5 Kreiranje lastnega para ključev

Postopek generiranja lastnega para ključev je precej preprost. V osnovi morate le zagnati `gpg -gen-key` . Kakorkoli, priporočam vam, da ustvarite tudi preklicni certifikat (revocation certificate) za vaše ključe v primeru, da kdaj izgubite dostop do vašega skrivnega ključa (npr. izgubite geslo zanj ali izgubite sam skrivni ključ). Navodila za kreiranje preklicnega certifikata najdete v poglavju *3.7* tega dokumenta.

Navodila spodaj so napisana korak za korakom, z varnostjo v mislih. Naprimer:

- ključe se generira z največjo možno velikostjo ključev, da se jih naredi bolj odporne na "brute force"napad
- ključi se generirajo z omejeno življenjsko dobo, da se prepreči njihova dolgoročno ogrožanje z vedno napredujočo računalniško tehnologijo
- ključe se shrani na disketnik, da se prepreči kraja ključev v primeru, da si nekdo pridobi dostop do vašega računalnika (z oddaljenega ralunalnika ali fizično)
- preklicni certifikat se generira, da se lahko javni ključ v primeru kompromiranja ali izgube ključa lahko prekliče

Nekateri ljudje, se bodo počutili varne tudi brez vseh teh varnostnih ukrepov. Naprimer, da posedujete prenosnik ali domač računalnik na katerem berete vso elektronsko pošto, se lahko počutite dovolj varno, da na disku tega računalnika shranite vaš par ključev. Lahko tudi varno generirate par ključev katerega veljavnost nikdar ne poteče in katerega lahko uporabljate za identifilacijo in večino komunikacij - ter kreirate še par ključev, ki ga uporabljate za izjemno občutljive komunikacije (če imate kake). Ponovno navodila, ki si sledijo korak za korakom spodaj so napisana z mislijo na čim boljšp varnost. Ni vam jih nujno potrebno slediti, da generirate par ključev. Po drugi strani, le ste izjemno paranoični varnostni "freak"kot sem jaz potem vam bo sledenje spodnjim navodilom prineslo občutek pomirjenosti, ki ga trenutno ***tako*** potrebujete.

1) Pojdite na www.gnupg.org, ter k sebi na disk shranite zadnjo verzijo gnupg-ja: gnupg-x.x.x.tar.gz

Opozorilo: Prepričajte se, da imate dejansk vsaj verzijo GnuPG-ja 1.0.6, ker verzije pred to imajo pomembne varnostne luknje v njih.

2) Preverite PGP podpis ter MD5 vsoto GnuPG arhiva:

```
[vab@firster vab]$ gpg --verify gnupg-x.x.x.tar.gz.sig gnupg-x.x.x.tar.gz
[vab@firster vab]$ md5sum gnupg-x.x.x.tar.gz
```

3) Razpakirajte arhiv, ga skonfigurirajte, prevedite ter inštalirajte:

```
[vab@firster vab]$ tar xvzf gnupg-x.x.x.tar.gz
[vab@firster vab]$ cd gnupg-x.x.x
[vab@firster gnupg-x.x.x]$ ./configure
[vab@firster gnupg-x.x.x]$ make
[vab@firster gnupg-x.x.x]$ su
[vab@firster gnupg-x.x.x]# make install
[vab@firster gnupg-x.x.x]# exit
[vab@firster gnupg-x.x.x]$ cd
```

Če delite sistem na katerega inštalirate GnuPG še z kom, bi morda želeli GnuPG narediti setuid root, tako, da lahko uporablja zaščiten spomin. Če to želite storiti, priporočamo previdnost da preverite vaš arhiv z md5 podpisom, ter pgp podpisom, da si zagotovite da ni trojanski konj.

4) Najdite disketo, na katero boste shranili ključe, ter jo sformatirajte.

```
[vab@firster vab]$ /sbin/mkfs.ext2 /dev/fd0
```

4a) "Mount-ajte"disketno enoto ter naredite direktorij, ki pripada vam na njej za vaše ključe:

```
[vab@firster vab]$ mount /mnt/floppy
[vab@firster vab]$ mkdir /mnt/floppy/.gnupg
```

ter če je potrebno (odvisno od dostopa do fd0 na vašem sistemu):

```
[vab@firster vab]$ chown <vaš_uid>:<vaš_gid> /mnt/floppy/.gnupg
```

4b) Naredite symlink z vašega domačega direktorija na disketo

```
[vab@firster vab]$ ln -s /mnt/floppy/.gnupg .gnupg
```

5) Generirajte svoje gnupg ključe

```
[vab@firster vab]$ gpg --gen-key
```

5a) Izberite tip ključa, ki ga želite - Privzeto je v redu.

```
Please select what kind of key you want:
(1) DSA and ElGamal (default)
(2) DSA (sign only)
(4) ElGamal (sign and encrypt)
Your selection? <return>
```

5b) Izberite velikost svojega ključa: 2048

```
DSA keypair will have 1024 bits.
About to generate a new ELG-E keypair.
minimum keysize is  768 bits
default keysize is 1024 bits
highest suggested keysize is 2048 bits
What keysize do you want? (1024) 2048<return>
Do you really need such a large keysize? yes<return>
```

5c) Nastavite življenjsko dobo tega ključa: 5 let je v redu

```
Requested keysize is 2048 bits
Please specify how long the key should be valid.
0 = key does not expire
<n>  = key expires in n days
<n>w = key expires in n weeks
<n>m = key expires in n months
<n>y = key expires in n years
Key is valid for? (0) 5y<return>
Key expires at Sun Sep 21 16:17:15 2005 EDT
Is this correct (y/n)? y<return>
```

5d) Vnesite svoje ime/priimek ter elektronsk(i/e) naslov(e)...

```
Real name: Demo User<return>
Email address: demo@nonexistent.nowhere<return>
Comment:
You selected this USER-ID:
"Demo User <demo@nonexistent.nowhere>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?  O<return>
```

5e) Izberite si geslo. Izbrati morate dobro geslo. Bilo naj bi dolgo, ter težko za uganiti. Mora biti nekaj, česar ne boste pozabili. Če pozabite svoje geslo ne morete več uporabljati ključa.

5f) Premikajte miško, ter pritisnite nekaj tipk, morda posodobite locate ali naredite večje iskanje z find ukazom. GPG bere iz /dev/random, da dobi več naključnosti za generacijo vaših ključev. /dev/random v glavnem naseljujejo prekinitve.

6) Spremenite svoj ključ, če to želite. Na primer, če imate več elektronskih naslovov in jih želite vse kot veljavne na vaših ključih:

```
[vab@firster vab]$ gpg --list-secret-keys

/home/vab/.gnupg/secring.gpg
----------------------------
sec  1024D/C01BAFC3 2000-09-21 Demo User <demo@nonexistent.nowhere>
ssb  2048g/7A4087F3 2000-09-21
[vab@firster vab]$ gpg --edit-key C01BAFC3
Command> help
Command> adduid
[...]
Command> save
```

7) Pošljite vaš ključ na strežnik s ključi

```
[vab@firster vab]$ gpg -keyserver <strežnik_s_ključi> -send-key <Vaš_Key_ID>
```

Videti bi morali sporočilo o uspehu kot je tole:

```
gpg:  success sending to '<strežnik_s_ključi>' (status=200)
```

Tu je pomembno omeniti, da nekateri ljudje verjamejo, da skrivanje ključev (shranjevanje le teh brez objave) pripomore k dodatni varnosti za njihove enkriptirane komunikacije. To je res, ker na strežniku s ključi bi lahko prišlo do vdora ali kompromizacije in vrnili napačen javni ključ, ko bi bil le-ta zahtevan. Nadalje, ključ ma določenem javnem strežniku s ključi morda ni najnovejša verzija ključa. Naprimer dodatni podpisi so morda bili dodani ključu, ki ni bil poslan na strežnik s ključi. To je tudi res ker je za določene tipe napadov na javni enkripcijski sistem, ki ga uporablja PGP potreben javni ključ. Medtem, ko mnogo ljudi pričakuje, da z razumno velikimi ključi ti napadi nebi mogli biti uspešni, tako da je vseeno, ali je javni ključ objavljen, ohranjanje javnega ključa v tajnosti dejansko ojača par ključev.

Jaz ne priporočam da ohranite svoj javni ključ v tajnosti, ker bo to druge odvrnilo od uporabe PGP-ja v njihovih komunikacijah z vami. Če se znova dotaknemo teme o možnosti pokvarjenega ali kompromiranega strežnika s ključi, ki bi vračal napačne ključe, se lahko zaščitite pred tem, da bi vam pošiljali sporočila z pokvarjenimi ključi, tako, da objavite fingerprint svojega ključa v svoji .signature datoteki ali na spletu. Da se posvetimo temi napada vašega para ključev preko dosegljivosti vašega javnega ključa bi rekel, če ste resnično zaskrbljeni glede čvrstosti vašega para ključev ali resnično paranoični glede varnosti vaših komunikacij, lahko generirate dodatne pare ključev (ki potečejo v roku ur ali dni) za vsako komunikacijo ter izmenjate javne ključe teh parov skozi kodirane komunikacije z posamezniki s katerimi želite komunicirati.

Če ne želite imeti svojega ključa na javnem strežniku s ključi lahko preskočite ta korak ter namesto tega pošljete svoj javvni ključ koordinatorju srečanja z sporočilom v katerem napišete, da svojega javnega ključa ne želite imeti na javnem strežniku s ključi. Koordinator lahko prebere informacije o vašem ključi ter posreduje vaš ključ ostalim udeležencem srečanja preko kodirane elektronske pošte, ali kake druge metode, poleg tega pa še sporočilo, da naj se ključ po podpisu vrne lastniku, in se ne pošlje na strežnik s ključi.

8) Generirajte preklicni certifikat. To je neobvezen korak.

Generiranje in shramba preklicnega certifikata vam bo omogočila preklic vašega javnega ključa tudi v primeru da to le tega izgubite dostop zaradi kompromizacije, zaplembe, pozabljenega gesla, ali okvare medija na katerem je bil shranjen. Če želite imeti možnost, da prekličete vaš javni ključ kadar nimate dostopa do vašega skrivnega ključa, generirajte preklicni certifikat ter ga shranite na varnem mestu. Kopijo preklicnega certifikata je pametno natisniti, da ga lahko vseeno vnesete v primeru, da se vam okvari medij na katerem je bil shranjen.

Če pride do kompromizacije vašega preklicnega certifikata, bi dobil posameznik, ki je kompromiziral vaš certifikat možnost uporabe certifikata in potemtakem onemogočiti vaš ključ. Vendar, posameznik ne bo mogel kompromirati vašega skrivnega ključa preko preklicnega certifikata. Torej ne bo zmožen ustvariti ponarejenih podpisov, odkodirati sporočil zakodiranih z vašim parom ključev ali se predstavljati z njim za vas, kot lastnik vaših ključev. Ker je edini možni izid kompromizacije preklicnega certifilata onemogočenje vašega para ključev je v glavnem varna in pametna odlolitev.

Zopet oddelek *3.7* vsebuje več informacij o preklicu ključev.

GnuPG ukaz, ki generira preklicni certifikat je:

```
[vab@firster vab]$ gpg -output revcert.asc -gen-revoke <key_id>
```

9) Preko elektronske pošte pošljite podatke o vaših ključih koordinatorju srečanja, ter mu povejte, da pridete na srečanje. Ukaz napisan spodaj bo izpisal podatke, ki jih morate poslati koordinatorju, če uporabljate strežnik s ključi. Te podatke nato lahko pošljete v enkriptiranem sporočilu preko elektronske pošte koordinatorju.

```
[vab@firster vab]$ gpg -fingerprint <Your_Key_ID>
```

10) Od-"mountajte"disketo ter jo izvrzite:

```
[vab@firster vab]$ umount /mnt/floppy
```

Opomba: Disketo lahko nsoite s seboj za dodatno varnost, ali pa jo lahko pustite v varnem zaklenjenem predalu mize, itd. Svojih ključev NOČETE imeti v .gnupg direktoriju, ki je dosegljiv preko spleta.

11) Prikažite se na srečanju.

3.6 Podpisovanje ključev ostalih

1. korak: Dobite kopijo ključa

Navadno boste delali z strežnika s ključi. Toda če ključ, ki ga podpisujete ni disegljiv na strežniku s ključi ga lahko enostavno uvozite z ukazom

`gpg -import datoteka_z_javnim__ključem .`

Če pa delate z strežnikom s ključi, pa bo naslednji ukaz shranil ključ s strečnika v vaš javni keyring

`[vab@firster vab]$ gpg -keyserver <strežnik_s_ključi> -recv-keys <Key_ID>`

Če dobite napako za branje, to pomeni da so strežniki s ključi preobremenjeni. Prosim poskusite znova čez nekaj sekund.

2. korak: Poglejte fingerprint ključa in ga overite

`[vab@firster vab]$ gpg -fingerprint <Key_ID>`

GPG bo izpisal podatke o ključu (katerega ste ravnokar shranili s strežnika s ključi): fingerprint in <Key_ID >. Preverite, če se fingerprint shranjenega ključa ujema z fingerprintom ključa na vašem spisku, ki ste ga dobili na srečanju. Opozorilo: ne preverjajte fingerprinta na spletni strani strežnika s ključi, ker ni nujno da bam bo poslal isti ključ, kot je prikazan na spletni strani.

3. korak: Podpišite ključ

`[vab@firster vab]$ gpg -sign-key <Key_ID>`

Če imate več privatnih ključev določite s katerim ključem želite podpisati z ukazom podobmin temule:

`[vab@firster vab]$ gpg -default-key <Ključ_ki_ga_boste_uporabili> -sign-key <Key_ID>`

Če imate probleme z delom z RSA ključi po vsej verjetnosti uporabljate staro verzijo gnupgja. Verzije GnuPG-ja starejše od 1.0.3 ne vsebujejo podpore za RSA algoritem. Opozorilo: morda morate odstraniti starejšo verzijo, ki jo je vašo distribucijo namestila z orodjem za delo s paketi. Verzijo programa, ki ga kličete lahko preverite z sledečim ukazom:

`[vab@firster vab]$ gpg -version`

4. korak: Vrnite ali pošljite na strežnik s ključi podpisan ključ

Če delate z osebo, ki noče imeti svojih ključev na javnem ku s ključi, bi jim morali pri tem koraku vrniti njihov javni ključ preko metode po njihovi izbiri - navadno preko enkriptirane elektronske pošte. Javnega ključa ne smete poslati na javni strežnik s ključi brez dovoljenja njegovega lastnika. Objava javnega ključa malce zmanjša varnost para ključev, zatorej bi se razumelo kot nevljudno, če bi ključ naredili bolj javen, kot želi njegov lastnik.

Najverjetneje boste delali preko strežnika s ključi. V tem primeru lahko pošljete ključ na strežnik s ključi na sledeč način:

`[vab@firster vab]$ gpg -keyserver <strežnik s ključli> -send-key <Key_ID>`

Videti bi morali sporočilo podobno temu:

`gpg: success sending to '<strežnik_s_ključi>' (status=200)`

Čestitke, podpis ključa druge osebe je sedaj končan in vaš podpis je bil dodan v njihov javni ključ. Pot zaupanja je bila vzpostavljena.

3.7 Preklic vašega para ključev

V primeru, da sumite, da je bil vaš skrivni ključ kompromiran, bi morali takoj preklicati vaš javni ključ. Preklic ključa poteka z dodatkom preklicnega certifikata javnega ključa. Preklic ključa da vedeti, da ključ ni več veljaven (varen) in da se ga naj ne uporablja. Enkrat, ko je preklicni certifikat izdan, se ga ne da več preklicati.

Ker je vaš PGP ključ distribuiran (brei kroži) med ljudmi in se ne ureja z centralne točke morate distribuirati preklicni certifikat na isti način kot razširjate vaš javni ključ. Kroženje preklicnega certifikata na isti način kot vaš javni ključ bi navadno pomenilo, da preklicni certifikat pošljete na strežnike s ključi. Če ključa niste poslali na strežnik s ključi lahko kljub temu pošljete preklicni certifikat nanj (v tem primeru bi se poznala razlika med prosto dostopnostjo javnega ključa in nezmožnostjo opozorila oseb da je bil vaš ključ preklican).

Ponovno, ukaz za kreiranje preklicnega certifikata je sledeč:

```
[vab@firster vab]$ gpg -output revcert.asc -gen-revoke <key_id>
```

Če se vam dozdeva kdaj in kako je plišlo do komprimizacije vašega ključa in ste generirali preklicni certifilat med generacijo ključa, boste lahko še vedno generirali nov preklicni certifikat, za preklic vašega para ključev, to pa zato, ker vam openPGP omogoča, da opišete razlog preklica, ter napišete še nekaj teksta o tem zakaj ključ preklicujete. Kroženje takšnega preklicnega certifikata ima svoje prednosti in je bolj zaželjeno kot kroženje splošnega preklicnega certifikata generiranega med kreiranjem ključev.

4 Pomembni podatki, ter viri za za več informacij

4.1 Spisek javnih strežnikov s ključi

1. *CryptNET Omrežje strežnikov s ključi*
   (a) *gnv.keyserver.cryptnet.net*
2. *www.keyserver.net Omrežje*
   (a) *search.keyserver.net*
   (b) *seattle.keyserver.net*
   (c) *germany.keyserver.net*
   (d) *belgium.keyserver.net*
   (e) *finland.keyserver.net*
   (f) *thailand.keyserver.net*
3. *pgp.ai.mit.edu*
4. *pgp.uni-mainz.de*

5 Povezave na sorodne dokumnte

GnuPG FAQ (en)

GnuPG Prirośnik (en)

GnuPG Mini Howto (English)

comp.security.pgp FAW

5.1 Povezane spletne strani

GnuPG Domača Stran (en)

Domača stran združenja OpenPGP (en)

Mednarodna domača stran PGP (en)

Stran izrisovanja grafov Debian (en)

Programski paket AT&T Labs-Research Graphviz (en)

Stran o sledenju podpisov (en)

5.2 Povezani RFC-ji

rfc2440

6 O tem dokumentu

Ta dokument živi na naslovu *http://www.cryptnet.net/fdp/crypto/gpg-party.html*

Prevedel 23.12.2001 Boštjan Müller

6.1 Verzije

Version 1.0.0, 2000.10.01 Začetna izdaja

Version 1.0.1, 2000.10.03 Spremembe v načinu pisanja, informacije o javnih ključih

Version 1.0.2, 2000.12.07 Popravljena napaka v povezavi

Version 1.0.3, 2001.01.14 Poenostavitve, Risanje grafov, Obnašanje in varnost na strežnikih s ključi, Perl koda, Primeri objav, Dodatni podatki, splošni popravki

Version 1.0.4, 2001.06.21 Podatki o preklicnih certifikatih dodani: 3.5, 3.7. RFC informacije dodane: 4.4. Spisek strežnikov s ključi ter povezave na spletne strani posodobljene.

6.2 Sodelavci

V. Alex Brennen (Glavni avtor)

John Sheehy (Tehnični predlogi, primeri objav)

Darxus (Popravki HTML-ka, primeri poenostavitev, Koda za delanje grafov (sig2dot.pl & sigtrace.pl))

Peter Palfrader (Tehnični predlogi, Obnašanje na strežnikih ključev, dodatni predlogi)

Ryan Brouillard (Primer brošure za tisk)

Jeremy Scofield (Predlogi za način pisanja/format)