

GPG/PGP-opas

GNU Privacy Guard (GPG tai GnuPG) on vapaa versio tiedostojen salaamiseen ja allekirjoittamiseen tarkoitetusta PGP-ohjelmasta. Siitä on saatavissa versiot Linuxin lisäksi myös Windowsille, GNU Hurdille, BSD:ille, MacOS X:lle, VMS:lle ja PocketPC:lle.

Kaikki oppaassa mainitut ohjelmat löytyvät VALO-CD:ltä: Mozilla Thunderbird, GPG ja Enigmail.

Salaiset ja julkiset avaimet

GPG:ssä käytetään kahdenlaisia avaimia, salaisia ja julkisia. Kuten nimistä voi päätellä, julkinen avain on tarkoitettu levitettäväksi julkisesti tai esimerkiksi lähetettäväksi avainpalvelimelle ja salainen avain on tarkoitus pitää vain käyttäjän omassa käytössä.

Kun käyttäjällä on toisen henkilön julkinen avain tämä voi salata viestin (tai tiedoston) siten, että sen avaamiseen tarvitaan vastaanottajan salainen avain. Vastaavasti salaista avainta käyttämällä on mahdollista lisätä viestiin allekirjoitus, jonka aitouden voi tarkistaa julkisella avaimella.

Salaista avainta käytettäessä tarvitaan myös avaimen salasana.

Käyttö

GPG:tä käytetään komentoriviltä, mutta sille on olemassa myös graafisia käyttöliittymiä, kuten VALO-CD:llä mukana oleva Mozilla Thunderbiriin asennettava lisäosa nimeltä Enigmail.

Avainparin luominen

GPG:n asennuksen jälkeen ensimmäinen toimenpide on avainparin luominen (tai olemassa olevan tuominen). Avainpari luodaan, mikäli mahdollista paikallisella koneella verkko alhaalla, komennolla

```
$ gpg --gen-key
```

Tämän jälkeen gpg kysyy, minkä tyyppinen avain luodaan ja kuinka suuri avain (bitteinä) luodaan. Oletusasetukset ovat hyvät. Seuraavaksi kysytään, kuinka pitkään luotava avain on voimassa. Oletuksena avain ei vanhene koskaan mikä on usein hyvä vaihtoehto:

Valitse millaisen avaimen haluat:

- (1) DSA ja ElGamal (oletus)
- (2) DSA (vain allekirjoitus)
- (5) RSA (vain allekirjoitus)

Valintasi? 1

DSA-avainparissa tulee olemaan 1024 bittiä.

ELG-E keys may be between 1024 and 4096 bits long.

Minkä kokoisen avaimen luodaan? (2048)

Halutun avaimen koko on 2048 bittiä

Kuinka kauan avaimen tulee olla voimassa.

0 = Avain ei vanhene koskaan

<n> = Avain vanhenee n päivän kuluttua

<n>w = Avain vanhenee n viikon kuluttua

<n>m = Avain vanhenee n kuukauden kuluttua

<n>y = Avain vanhenee n vuoden kuluttua

Avain on voimassa? (0)

Avain ei vanhene koskaan

Onko tämä oikein? (y/N) y

Näiden tietojen jälkeen gpg kysyy nimen, kommentin ja sähköpostiosoitteen luotavaa avainta varten. Kommenttina voi olla vaikka privat, work tai home. Skandinaavisten ja muiden erikoismerkkien käyttö annetuissa arvoissa voi tuoda myöhemmin ongelmia. Real nimen lisäksi avainpariin voi myöhemmin lisätä muita aliavaimia (identiteettejä, sähköpostiosoitteita), joten voit käyttää samaa avainta monella sähköpostitunnuksella.

Oikea nimi: Pertti Peruskäyttäjä

Sähköpostiosoite: pera@linux.fi

Huomautus: Ensimmäinen GPG-avaimeni

Käytät merkistöä "utf-8".

Valitsit seuraavan käyttäjätunnuksen:

"Pertti Peruskäyttäjä <pera@linux.fi>"

Muuta (N)imi, (H)uomautus, (S)ähköposti vai (0)k/(L)opeta? 0

Nyt salaiselle avaimelle pyydetään salasana. Voit käyttää salasanan keksimiseen apuna ohjelmaa pwgen. Salasana suojaa hiukan salaista avainta jos se hukkuu tai joku saa kopion siitä käsiinsä.

Tarvitset salasanan suojaamaan salaista avaintasi.

Syötä salasana: [tarPEKs1_randoomi15salasana]

Toista salasana: [tarPEKs1_randoomi15salasana]

Näiden tietojen antamisen jälkeen kone luo varsinainen avainparin. Se voi kestää hetken ja jopa pysähtyä hetkeksi, jos tietokoneella ei tehdä muuta, sillä GPG tarvitsee satunnaisdataa riittävän turvallisten avainten luomiseksi. Satunnaisdataa saadaan seuraamalla käyttäjän enemmän tai vähemmän satunnaisia toimintoja koneella. Avainparin luomisen pysähtyessä saat ilmoituksen

Tarvitaan paljon satunnaislukuja. Voit suorittaa muita toimintoja (kirjoittaa näppäimistöllä, liikuttaa hiirtä, käyttää levyjä) alkulukujen luomisen aikana, tämä antaa satunnaislukugeneraattorille paremmat mahdollisuudet kerätä riittävästi entropiaa.

Tässä tapauksessa liikuttele hiirtä tai selaa wikiä, jotta satunnaislukugeneraattori sekoittuu tarpeeksi.

Kun kaikki tämä on tehty, gpg tulostaa tiedot juuri luodusta avaimesta, allekirjoittaa julkisen avaimen salaisella avaimella (itsellään) sekä lisää sen korkeimmalle luottamustasolle (ultimate) avainrenkaaseen trustdb.gpg, joka luodaan, jos sitä ei vielä ole olemassa.

```
gpg: key 7AF6D4B4 marked as ultimately trusted
julkinen ja salainen avain on luotu ja allekirjoitettu.
```

```
gpg: tarkistetaan trustdb:tä
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
pub 1024D/7AF6D4B4 2007-08-12
    Key fingerprint =
    6C00 8FC4 274D 441E F220 03F4 14D6 E291 7AF6 D4B4
uid                               Pertti Peruskayttaja <pera@linux.fi>
sub 2048g/49EF6931 2007-08-12
```

Tässä 7AF6D4B4 on avaimen tunnistenumero, jolla avaimeen tullaan myöhemmin viittaamaan. 1024 salauksen pituus (bittinä), D tarkoittaa että avain on DSA-algoritmillä luotu ja 6C00 8FC4 274D 441E F220 03F4 14D6 E291 7AF6 D4B4 on avaimen sormenjälki. Viimeisellä rivillä on avaimen luontipäivä.

Kaikki käytössä olevat avainparit näet komennolla

```
$ gpg --list-keys
```

Nyt avain on luotu ja allekirjoitettu itsellään (allekirjoituksista lisää myöhemmin). Tässä vaiheessa kannattaa luoda avaimen mitätöintitiedosto ja varmuuskopioida tämän jälkeen sekä äsken luotu salainen avain että mitätöintitiedosto varmaan paikkaan. Seuraavaksi käydään läpi miten tämä tapahtuu.

Avaimen mitätöintitiedosto

Avainta luotaessa kannattaa samalla luoda tiedosto, jolla on mahdollista mitätöidä avain. Jos esimerkiksi tulevaisuudessa unohdat avaimen salasanan tai avainparin salainen osa joutuu väriin käsiin, on avain mahdollista mitätöidä avainpalvelimilta tällä tiedostolla.

Kumoamistiedoston luomiseen tarvitaan avaimen salainen osa ja sen salasana. Se tehdään komennolla

```
gpg --gen-revoke tunnistenumero
```

Esimerkiksi edellä luodulle avaimelle

```
gpg --gen-revoke 7AF6D4B4
```

Tämän jälkeen gpg kysyy syyn avaimen mitätöintiin ja kommentin mitätöinnille. Tämän jälkeen gpg tulostaa mitätöintiosan muodossa

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
ohjelman versio ja muita tietoja
pitkä mystinen merkkisarja
-----END PGP PUBLIC KEY BLOCK-----
```

Tallenna tämä osa esimerkiksi CD-levylle. Lisäksi se kannattaa varmuuden vuoksi tulostaa.

Mitätöintitiedostolla avain voidaan sitten poistaa esimerkiksi julkiselta

avainpalvelimelta. Ohjeet tähän löytyy yleensä palvelimen kotisivulta.

Avainten tuominen ja vieminen

Jotta GPG:n salauksista ja allekirjoituksista saataisiin jotain hyötyä, on käyttäjien pystyttävä antamaan julkisia avaimiaan toisilleen.

Tietyn avaimen julkinen osa voidaan tallentaa tiedostoon komennolla

```
gpg --export -a tunnistenumero > tiedosto.key
```

Valitsin -a ei ole pakollinen, mutta se tallentaa avaimen teksti- eikä binäärimuodossa, jolloin se on selkeämpi lukea ja riski sen korruptoitumiseen on pieni.

Tällä tavalla tallennettu tiedosto voidaan tuoda toisessa GPG:ssä käyttöön komennolla

```
gpg --import avain.key
```

Julkisen avaimen voi julkaista vaikka kotisivullaan tai kantaa USB-tikulla. Avain voidaan myös lähettää julkisille avainpalvelimille, mutta ennen avaimen lähetystä kannattaa harjoitella ensin jonkun aikaa sen käyttöä, sillä avaimen luonnissa tapahtunutta virhettä ei voi korjata sen jälkeen, kun avain on julkistettu avainpalvelimilla. Sen voi julkaisun jälkeen ainoastaan mitätöidä, jos salainen avain on vielä tallessa, tai jos mitätöintitiedosto on muistettu luoda etukäteen ja se on hyvä tallessa. Avaimen julkaiseminen avainpalvelimelle käsitellään myöhemmin tässä artikkelissa.

Vastaanottaja voi tarkistaa avaimen todenperäisyyden, mikäli hänellä on tiedossa avaimen sormenjälki, joka on mieluiten saatu jotain muuta, kuin sähköistä reittiä pitkin. Hyviä siirtovälineitä ovat paperimuoto tai tarpeen vaatiessa puhelin. Sormenjälki on avaimestasi tiivistealgoritmilla laskettu 40-merkkinen merkkijono joka varmistaa, että elektronisesti välitetty avain ei ole muuttunut siirron aikana ja että se todella vastaa väitettyä avainta. Sormenjäljen tarkistaminen on se tapa, jolla ihminen pystyy järkevällä resurssinkäytöllä varmistamaan elektronisen avaimen liitettäessä sitä omaan julkisten avainten renkaaseen ja antamaan tälle luottotason.

Oman avaimen sormenjäljen saa selville komennolla

```
gpg --fingerprint tunnistenumero
```

Myös salaisia avaimia voidaan tallentaa tiedostoon. Tällöin käytetään valitsinta --export-secret-key:

```
gpg --export-secret-key -a tunnistenumero > salainen_avain.key
```

Salainen avain on syytä tallentaa ulkoiselle medialle (esim. CD-levylle) ja viedä levy paikkaan, josta se ei varmasti joudu vääriin käsiin. Vaikka salaista avainta suojaa avainta luotaessa valittu salasana, tämä suojaus ei ole niin vahva, että se estäisi varmasti salaisen avaimen väärinkäytökset.

Salainen avain voidaan tuoda käyttöön samaan tapaan kuin julkinenkin avain

komennolla `gpg --import avain.key`.

Viestien salaaminen ja purkaminen

Tämän jälkeen viestin salaaminen onnistuu valitsimen `-e` (tai `--encrypt`) avulla:

```
gpg --encrypt tiedosto
```

Jolloin GPG luo tiedoston `tiedosto.gpg` jossa tiedoston sisältö on salattuna. Tämän jälkeen GPG kysyy, millä julkisella avaimella viesti salataan (listan näet komennolla `gpg --list-keys`). Jos esimerkiksi halutaan salata tiedosto käyttäen yllä luodun avaimen julkista osaa, annetaan avaimen tunnuksiksi avaimen tunnistenumero `7AF6D4B4` ja painetaan enteriä. Avaimen tunnistenumero voidaan antaa myös valitsimella `-r`:

```
$ gpg -e -r 7AF6D4B4 tiedosto
```

Salattu viesti puretaan vastaavasti valitsimen `--decrypt` avulla:

```
gpg --decrypt tiedosto.gpg
```

Jolloin GPG kysyy avaimen kuuluvaa salasanaa. Avaimen salaisen osan on myös oltava käytettävissä.

Allekirjoittaminen

Allekirjoitettaessa tiedostoa annetaan gpg:lle valitsin `-s` (tai `--sign`) ja allekirjoitettava tiedosto:

```
$ gpg --sign tiedosto
```

Jonka jälkeen gpg pyytää salasanan ja allekirjoittaa tiedoston oletusavaimella. Jos halutaan käyttää jotain muuta kuin oletuksena käytettävää avainta, se voidaan antaa valitsimella `-u`:

```
$ gpg -s -u 7AF6D4B4 tiedosto
```

Tällöin tuloksen on tiedosto `tiedosto.gpg` jossa on allekirjoitettu viesti ja allekirjoitus pakattuna. Pakkaamattomana tiedosto allekirjoitetaan valitsimella `--clearsign`:

```
$ gpg --clearsign tiedosto
```

Jonka jälkeen tiedoston `tiedosto.asc` sisältö on seuraavanlainen:

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1
```

Moi

```
Terveiset linux.fi-wikille  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.4.6 (GNU/Linux)
```

```
iD8DBQFGvza7FNbikXr21LQRALZpAKCLpxonnAAT5A8szsRXKkRy04mNoQCfUbe+
GFHRIF6LK6UnPxYVcoTdSC0=
=hZ5I
```

Allekirjoituksen saa tallennettua erilliseen tiedostoon valitsimella `-b`. Tämä on kätevää etenkin allekirjoitettaessa binääritiedostoja:

```
$ gpg -b tiedosto
```

Jolloin tuloksena on tiedosto `tiedosto.sig` jossa on allekirjoitus pakattuna.

Allekirjoitus tarkistetaan antamalla `gpg`:lle valitsin `--verify`:

```
$ gpg --verify tiedosto
gpg: Signature made Sun 12 Aug 2007 19:35:07 EEST
      using DSA key ID 7AF6D4B4
gpg: Good signature from "Pentti Perussurffaaja <pera@linux.fi>"
```

Tällöin `gpg` siis kertoo, millä avaimella ja milloin allekirjoitus on tehty. Jos tiedostoa on muutettu allekirjoituksen jälkeen, toinen rivi muuttuu muotoon

```
gpg: BAD signature from "Pentti Perussurffaaja <pera@linux.fi>"
```

Jos allekirjoitus on erillisessä tiedostossa, annetaan se parametrina `gpg`:lle

```
$ gpg --verify tiedosto.sig
```

Avainpalvelimet

Avainpalvelimet ovat palvelimia, jonne käyttäjät voivat lähettää julkiset avaimensa ja josta muiden käyttäjien julkisia avaimia on mahdollista hakea.

Oma avain lähetetään avainpalvelimelle komennolla

```
$ gpg --keyserver palvelin --send-key tunniste
```

Esimerkiksi edellä luomamme avain lähetettäisiin palvelimelle `wwwkeys.eu.pgp.net` komennolla

```
$ gpg --keyserver wwwkeys.eu.pgp.net --send-key 7AF6D4B4
```

Vastaavasti tietty avain haettaisiin sieltä komennolla

```
$ gpg --keyserver wwwkeys.eu.pgp.net --recv-key tunniste
```

Joitain avainpalvelimia:

- `wwwkeys.eu.pgp.net`
- `wwwkeys.us.pgp.net`
- `pgp.dtype.org`
- `wveys.pgp.net`
- `search.keyserver.net`

Suurin osa avainpalvelimista on yhteydessä toisiinsa ja päivittää avaimet keskenään tietyin väliajoin. Siispä yleensä riittää, että lähettää avaimen vain yhdelle palvelimelle.

Avaimen mitätöiminen

Jos avain murretaan, salainen avain hukkuu tai avaimen käyttö muuten lopetetaan voidaan avainpalvelimelle lähettää tieto avaimen käytöstä poistamisesta **vain** mitätöintitiedoston avulla. Tästä syystä mitätöintitiedosto on tärkeää luoda avainparia luotaessa.

Mitätöintitiedosto lähetetään palvelimelle siten, että ensin se otetaan käyttöön gpg:lle ja tämän jälkeen avain lähetetään normaaliin tapaan avainpalvelimelle. Jos mitätöintitiedoston nimi olisi `avain.revoke`, se lähetettäisiin avainpalvelimelle seuraavasti:

```
$ gpg --import avain.revoke
gpg: key TUNNISTE: "Nimi <osoite>" revocation
      certificate imported
gpg: Kaikkiaan käsitelty: 1
gpg:   uusia avainten mitätöintejä: 1
--
$ gpg --keyserver avainpalvelin --send-key TUNNISTE
gpg: sending key TUNNISTE to hkp server avainpalvelin
```

Luottamusverkot ja avainten allekirjoittaminen

PGP-avaimella on siis mahdollista allekirjoittaa tiedostoja ja viestejä. Mutta miten vastaanottaja voi luottaa siihen, että allekirjoittaja on oikeasti se, kuka väittää olevansa? Tätä varten PGP-avaimia on mahdollista allekirjoittaa.

Allekirjoittaminen tarkoittaa sitä, että PGP:tä käyttävät henkilöt tapaavat toisensa ja tarkistavat toistensa henkilöllisyyden virallisella kuvallisella henkilöllisyystodistuksella (ajokortti, passi tms.) ja avaintensa sormenjäljet. Avaimen sormenjälki on tietyn avaimen tunnistemerkkijono. GPG:llä avainten sormenjäljet näkee komennolla

```
gpg --fingerprint
```

--fingerprint-valitsimen perään voi laittaa myös hakusanan, esimerkiksi

```
gpg --fingerprint henkilön nimi
```

Sormenjäljen käytön ideana on varmistaa, että allekirjoitettava avain on nimenomaan kyseisen henkilön oikea julkinen avain.

Nyt kun sinulla on toisen käyttäjän avaimen sormenjälki ja olet tarkistanut tämän henkilöllisyyden (henkilöllisyyden tulee toki vastata avaimen tiedoissa olevaa nimeä), voit allekirjoittaa henkilön avaimen seuraavasti:

- Tuo henkilön julkinen avain käyttäen joko avainpalvelimia tai lataamalla julkisen avaimen sisältävä tiedosto esim. kyseisen henkilön kotisivuilta
- Avaa avain muokattavaksi komennolla

```
gpg --edit-key tunniste
```

- Aukeavassa listassa on avaimen tiedot ja tämän jälkeen yksi tai useampi rivi tyyliin

[unknown] (1). Käyttäjän Nimi (kommentti) <sähköposti>

- Kirjoita *n*, jossa *n* on sulussa oleva numero. Valitse näin uid:t (sähköpostiosoitteet), jotka haluat allekirjoittaa. Enterin painaminen valitsee kaikki uid:t.
- GPG näyttää avaimen sormenjäljen ja salauksen vahvuuden. Tarkista, että tiedot ovat samat, jotka sait henkilöltä tapaamisen yhteydessä.
- Allekirjoita avain komennolla `sign`.
- Jos tarkistuksen huoleellisuutta kysytään, valitse "arkinen" (*casual*) (2).
 - Tämä numero on julkista tietoa ja kertoo, kuinka tarkkaan avainten vaihto on suoritettu. Taso 2 vastaa sitä, että henkilöllisyys on tarkistettu. Taso 3 tarkoittaa, että sähköpostin oikeellisuus on todettu.
- Poistu muokkaustilasta komennolla `quit`.

Avaimen allekirjoitukset näkee komennolla

```
gpg --list-sigs tunniste
```

Lopuksi allekirjoitettu avain voidaan lähettää takaisin sen omistajalle tallentamalla se normaalisti tiedostoon (`gpg --export -a tunniste > tiedostonimi`). Jos joku allekirjoittaa avaimesi, kannattaa se sen jälkeen lähettää avainpalvelimelle tavalliseen tapaan (`gpg --keyserver palvelin --send-keys tunniste`).

Lisätietoa tarkistustasosta 3

Mikäli haluat valita tarkistustasoksi korkeimman eli arvon 3, sinun tulisi lähettää allekirjoitettu (ali)avain kryptattuna vastaanottajan kyseiseen aliosoitteeseen. Tämä vastaa sitä, että tarkistat sähköpostiosoitteen toimivuuden. Jos vastaanottaja saa viestin auki, hän voi ottaa käyttöön tämän aliosoitteen allekirjoituksen. Tällöin allekirjoituksesi ilmestyy avaimen aliosoitteen kohdalle vasta, kun avaimen omistaja on päivittänyt avaimensa ja julkaissut sen. Ongelmaksi jää nyt se, että sinulle voi jäädä omaan avainrenkaaseen allekirjoitus, vaikka sinulla ei ole varmuutta, onko sähköposti voimassaoleva. Tähän auttaa se, että poistat ensin käyttäjän avaimen ja noudat sen vain avainpalvelimilta tai käyttäjän kertoman julkaisukanavan kautta.

Lähde ja lisenssi

Tämä artikkeli on sovitettu Linux.fi:n wikin artikkelista [GPG](#). Sisältö on käytettävissä lisenssillä Creative Commons 3.0 (Nimi mainittava).