

Enigmail-opas

Enigmail on Mozilla Thunderbird ja Mozilla Seamonkey -ohjelmille tehty liitännäinen GPG-salausohjelmiston käyttöä varten. Sitä käytetään etenkin Thunderbirdin kanssa sähköpostin salaamiseen ja allekirjoittamiseen.

Enigmail on saatavissa Linuxin lisäksi myös Windowsille.

Asennus

Enigmail-liitännäinen löytyy VALO-CD:ltä kansioista `ohjelmat` ja voit asentaa sen vetämällä tiedoston `enigmail-x.x.x-tb-win.xpi` avoimena olevaan Thunderbird-ikkunaan, jolloin lisäosan asennus käynnistyy automaattisesti.

Avainten hallinta

Seuraavassa käsitellään Enigmailin käyttöä Thunderbird-sähköpostiohjelman kanssa. Koska Enigmail on vain GPG:n käyttöliittymä, samat asiat olisi mahdollista tehdä myös komentoriviltä `gpg`-ohjelmalla. Lisäksi Enigmailissa tehdyt muutokset vaikuttavat myös itse GPG:hen. GPG:n käytöstä kerrotaan tarkemmin GPG-oppaassa.

Avainparin luominen

Uusi avainpari voidaan luoda Enigmaililla graafisesti valitsemalla Thunderbirdin päävalikossa *OpenPGP - Avainten hallinta*. Aukeavasta *OpenPGP-avainten hallintaikkuna* -ikkunasta valitaan *Luo - Uusi avainpari*.

Tällöin aukeaa uusi ikkuna, jossa avainpari luodaan. Avainparin tiliksi on valittava jokin Thunderbirdin sähköpostitili, jolloin avaimen henkilön nimeksi ja sähköpostiosoitteeksi tulee kyseisen tilin mukaiset tiedot. Tilejä voi luoda Thunderbirdin *Muokkaa - Tilien asetukset* -valikosta.

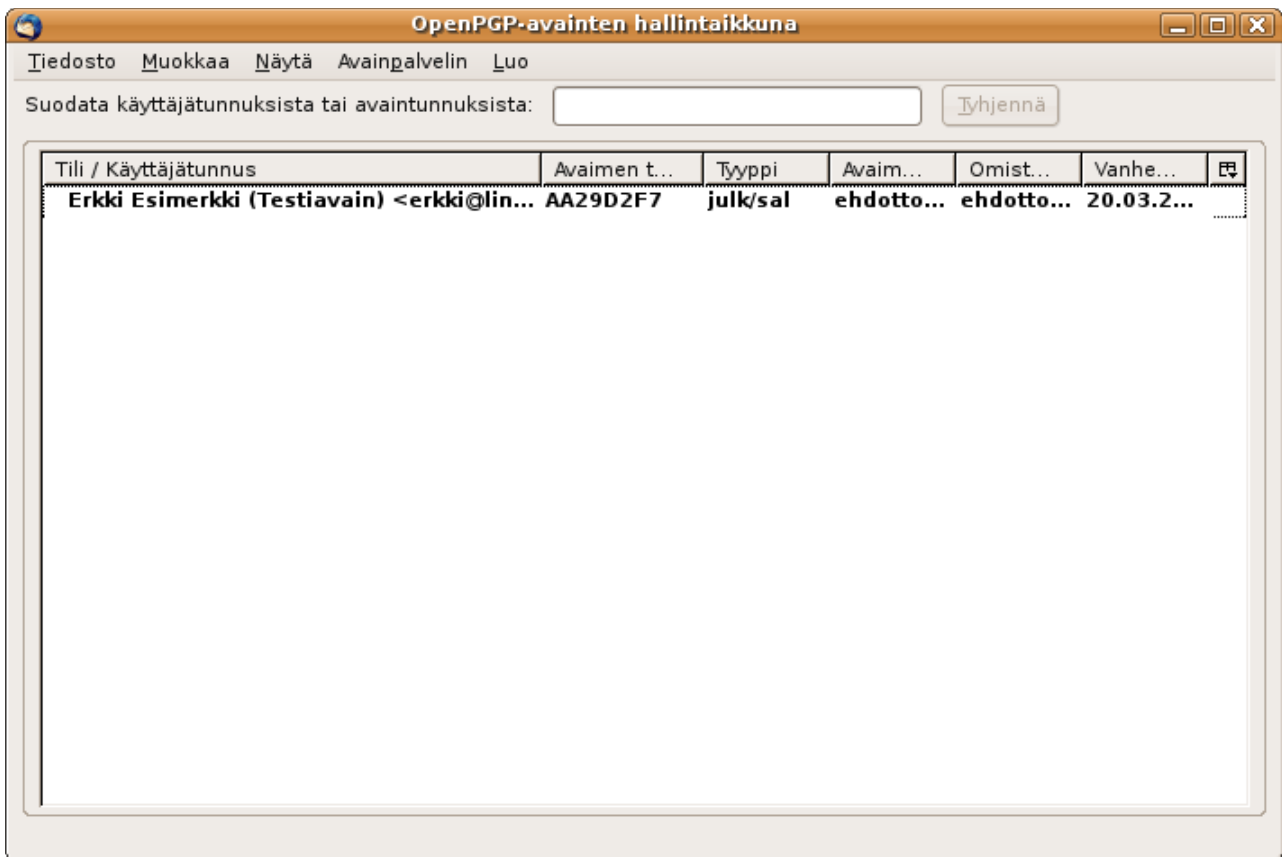
Avainparille on valittava tilin lisäksi myös salasana, kirjoitettava avainta koskeva kommentti ja asetettava sen vanhenemisaika. Kun tiedot on annettu, luodaan avain napsauttamalla *Luo avain* -painiketta. Avaimen luonti kestää jonkin aikaa ja sitä voi nopeuttaa käyttämällä tietokonetta esim. Linux.fin selailuun jolloin järjestelmä pystyy tuottamaan nopeammin riittävän satunnaisia satunnaislukuja.

Kun avain on luotu, Enigmail kysyy, luodaanko avaimelle mitätöintivarmenne. Varmenteen luominen on suositeltavaa, sillä sitä voidaan käyttää avaimen mitätöintiin jos alkuperäinen salainen avain hukkuu tai päättyy väärin käsiin. Mitätöintivarmenne on ainoa tapa poistaa avain julkisilta avainpalvelimilta!

Kysymykseen mitätöintivarmenteesta kannattaa siis vastata kyllä. Tämän jälkeen ohjelma kysyy tiedoston, johon varmenne tallennetaan. Varmenne kannattaa myöhemmin polttaa levyille ja jopa tulostaa.

Avainten hallintaikkuna

Nyt kun avain on luotu, se näkyy avainten hallintaikkunassa. Luotu avaimemme on tyyppiä *julk/sal*, sillä se luotaessa luotiin sekä salainen että julkinen avain. Lisäksi tässä ikkunassa näkyy mm. avaimen tunnistenumero, vanhenemispäivä ja luottamustaso.



Uuden tunnuksen lisäämien avaimeen

Avainta luotaessa sille asetettiin tietyn henkilön nimi ja sähköpostiosoite (käyttäjän tunnus). Yksi avain voi kuitenkin sisältää useampia tunnuksia. Yleensä käyttäjä lisää omaan avaimeensa kaikki käyttämänsä sähköpostiosoitteet - sähköpostiosoitteen vaihtuessa ei siis tarvitse vaihtaa GPG-avainta.

Uusi tunnus luodaan napsauttamalla avainta hallintaikkunassa hiiren oikealla painikkeella ja valitsemalla *Hallinnoi käyttäjätunnuksia*. Aukeavassa ikkunassa voidaan lisätä uusi tunnus *Lisää*-painikkeesta. Aukeavaan ikkunaan annetaan nimi (joka yleensä on sama), sähköpostiosoite ja kommentti ja painetaan *lisää*. Tämän jälkeen oletuksena käytettävä tunnus valitaan listasta ja napsautetaan *Aseta ensisijaiseksi* -painiketta.

Jos avaimelle on asetettu useampi tunnus, sen vieressä näkyy avainten hallintaikkunassa plus-merkki, jota napsauttamalla kaikki tunnukset tulevat näkyviin.

Julkisen avaimen vieminen

Avainparin julkinen avain voidaan tallentaa tiedostoon sen levittämistä varten. Tämä onnistuu napsauttamalla avainta avainten hallintaruudussa hiiren oikealla painikkeella ja valitsemalla *Vie avaimet tiedostoon*. Tämän jälkeen Enigmail kysyy, tallennetaanko tiedostoon myös salainen avain. Yleensä salaista avainta ei haluta viedä, joten tähän vastataan ei. Tämän jälkeen valitaan tiedosto, johon julkinen avain tallennetaan. Tallennuksen jälkeen julkisen avaimen sisältämän tiedoston voi laittaa jakoon esimerkiksi omille kotisivuille.

Jos edellä olleeseen kysymykseen vastaa myöntävästi, tiedostoon tallennetaan julkisen avaimen lisäksi myös salainen avain. Tämä on kätevää varmuuskopioitaessa avainta mutta *tämä tiedosto on ehdottomasti pidettävä tallella!*

Avaimen lähettäminen avainpalvelimelle



Paras tapa julkaista oma julkin avain on lähettää se julkiselle avainpalvelimelle josta muut käyttäjät voivat sen hakea esimerkiksi sähköpostiosoitteen tai nimen perusteella. Lähettäminen tapahtuu napsauttamalla avainten hallintaikkunassa lähetettävää avainta hiiren oikealla painikkeella ja valitsemalla *Siirrä julkiset avaimet avainpalvelimelle*. Aukeavassa ikkunassa voidaan valita avainpalvelin, jolle avaimet lähetetään. Yleensä riittää lähettää avain vain yhdelle palvelimelle, sillä yleisimmät julkiset avainpalvelimet kopioivat julkisia avaimia toisiltaan.

Avaimen hakeminen avainpalvelimelta

Toisten käyttäjien julkisia avaimia voi etsiä avainpalvelimelta valitsemalla *Avainpalvelin - Etsi avaimia*. Aukeavassa ikkunassa valitaan taas käytettävä avainpalvelin ja hakusana. Hakusana on tässä tapauksessa avaimen liitetty sähköpostiosoite, nimi tai tunnus

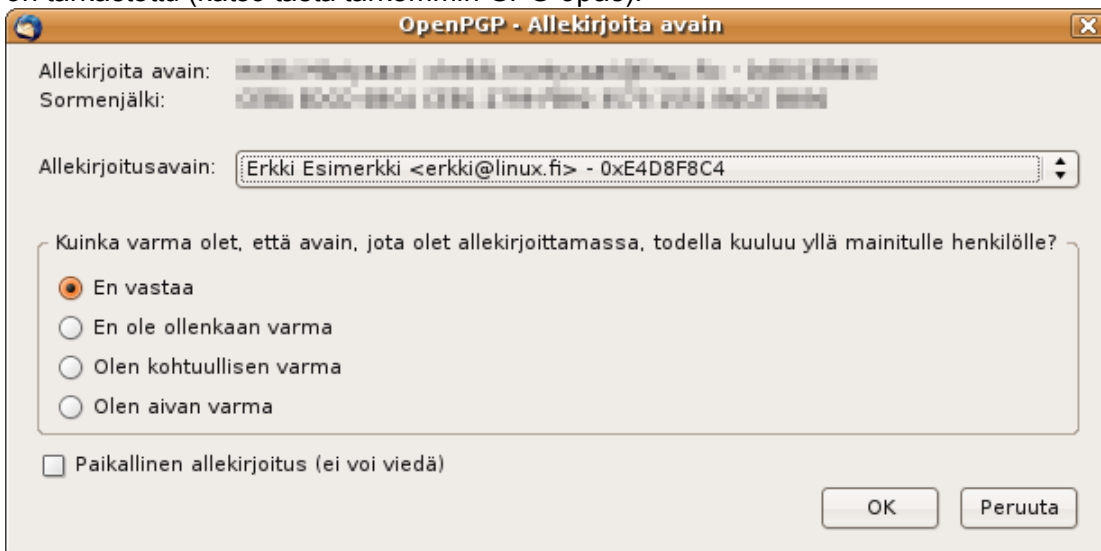
Haun jälkeen aukeaa ikkuna, jossa on listattu annettua hakusanaa vastaavat avaimet. Näistä halutut avaimet voidaan tuoda valitsemalla avaimet listasta ja painamalla OK-painiketta. Tällöin julkiset avaimet ladataan avainpalvelimelta ja ne ilmestyvät näkyviin avainten hallintaikkunaan.

Avaimen hakeminen tiedostosta

Julkisen (ja salaisenkin) avaimen voi tuoda järjestelmään myös tiedostosta valitsemalla avainten hallintaikkunassa *Tiedosto - Tuo avaimet tiedostosta* ja valitsemalla aukeavassa ikkunassa avaimen sisältävän tiedoston.

Avainten allekirjoittaminen

Myös avainten allekirjoittaminen on mahdollista Enigmaililla. Se tapahtuu napsauttamalla haluttua avainta hiiren oikealla painikkeella ja valitsemalla *Allekirjoita avain*. Aukeavassa ikkunassa valitaan allekirjoituksen vahvuus sen mukaan, kuinka tarkasti henkilön henkilöllisyys on tarkastettu (katso tästä tarkemmin GPG-opas).



Allekirjoituksen jälkeen on allekirjoitettu julkinen avain lähetettävä takaisin avaimen omistajalle jotta tämä voi julkaista uuden allekirjoitetun version avaimestaan. Avaimen palauttaminen on kätevä tehdä lähettämällä se salattuna sähköpostina avaimessa ilmoitettuun sähköpostiosoitteeseen jolloin tulee samalla varmistettua, että avaimessa oleva sähköpostiosoite kuuluu oikealle käyttäjälle.

Lisätietoja avaimen allekirjoittamisesta (mm. lista tarkistettavista asioista) löytyy GPG-oppaasta.

Sähköpostin salaus ja allekirjoittaminen

Enigmail mahdollistaa sähköpostien salaamisen ja allekirjoittamisen vaivattomasti.

Lähtettäminen

Kirjoitettaessa sähköpostia Thunderbirdillä voidaan viesti valita salattavaksi tai allekirjoitettavaksi kirjoitusikkunan työkalurivillä olevasta OpenPGP-painikkeesta. Kyseistä painiketta napsauttamalla aukeaa ikkuna, josta voidaan valita, allekirjoitetaanko ja salataanko viesti.

Jos viesti valitaan salattavaksi se salataan sillä koneelta löytyvällä julkisella avaimella, joka vastaa vastaanottajan sähköpostiosoitetta. Jos tällaista avainta ei löydy, Enigmail avaa uuden ikkunan jossa kysytään, millä avaimella viesti salataan. Tässä ikkunassa on myös *Nouda puuttuvat avaimet* -painike jolla voidaan etsiä kyseisen sähköpostiosoitteen omistajan julkista avainta avainpalvelimilta.

Vastaanottaminen

Vastaanotettaessa salattu viesti Enigmail kysyy automaattisesti salaisen avaimen salasanaa (edellyttäen toki, että salainen avain löytyy). Kun tämä salasana on annettu, näytetään viesti salaamattomana ja viesti-ikkunassa on OpenPGP-viesti *Viesti, jonka salaus on purettu*.

Vastaavasti vastaanotettaessa allekirjoitettu viesti Enigmail tarkistaa, vastaako allekirjoitus järjestelmästä löytyvää kyseiseen sähköpostiosoitteeseen liitettyä julkista avainta (jos tämä avain löytyy). Jos koneelle ei ole asennettu tarvittavia julkisia avaimia Enigmail mahdollistaa näiden etsimisen avainpalvelimelta.

Lisätietoja

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