Sisällysluettelo

- 1 (Open)PGP teemailta
- 2 Yleistä
- 3 ohjelmistot
- 4 esitiedot
    - 4.1 Asentaa saa omalle koneelle etukäteen
- 5 osallistujat
    - 5.1 HUOM

(Open)PGP teemailta

Tilassa järjestetään torstaina 9.8.2012 klo 18:00 alkaen PGP teemailta, jossa käydään PGP:n käyttökohteita GnuPG ohjelmalla läpi. Vetäjänä rostbach. Myöhemmin järjestään jatkoilta samaan teemaan.

Tapahtuma on avoin myös 5w:n ulkopuolisille jäsenille. Ovet aukeavat normaalisti soittamalla numeroon 0408166133 ja odottamalla hetki.

Yleistä

PGP (Pretty Good Privacy) on tarkoitettu suojaamaan (alunperin) yksityisten ihmisten yksityisyyttä. Eniten sitä käytetään sähköpostin allekirjoituksessa ja muokkaamisen estossa sekä salauksessa. Sitä voi myös käyttää myös muiden dokumenttien kanssa.

PGP hyödyntää toiminnassaan julkisen avaimen menetelmää (PKI), johon kuuluu oleellisena osana se, että avain on jaettu kahteen osaan; julkiseen ja yksityiseen (salaiseen) mikä tuo huikeita etuja tavalliseen yksityiseen avaimeen verrattuna.

Avainten hallinta on tärkeä osa PGP:tä, sillä siinä hyödynnetään Web-of-Trust:ia eli avainten avulla voidaan luoda luottamusketjuja toisiin avainhaltijoihin tekemällä niihin sähköisiä allekirjoituksia.

Oman PGP-avaimen luonti voidaan alusta asti suorittaa itsenäisesti, ilman 3. osapuolia turvallisesti. Tässä PGP eroaa esim. HST kortista, jossa vrk:n kautta käyttäjä saa valmiiksi luodun älykortin, joka sisältää yksityisen avaimen, eikä voi itse vaikuttaa siihen.

PGP:tä voi käyttää hyvin ilman luottamusominaisuuksia, mutta niitä voi myös halutessaan laajentaa tunnistautumalla toisten avaimenhaltijoiden kanssa henkilökohtaisesti ja vaihtamalla tiedot avaimien tiivisteistä. Tämä tapahtuu yleensä pienellä paperimedian vaihdolla (käyntikortti). Massatapahtumia, joissa usea henkilö vaihtaa yhdellä kertaa tunnistautumistietoja kutsutaan keysigning partyiksi.

ohjelmistot

Win: http://www.gpg4win.org/

Linux: gnupg (v.1.4 standalone, ei patentoituja algoritmeja) gnupg2 (modulaarinen, IDEA-algoritmi) molemmat voivat olla asennettu)

esitiedot

Ei pakollisia.

Suositeltavaa lukuaineistoa: http://linux.fi/wiki/Gpg

Asentaa saa omalle koneelle etukäteen

Win: http://www.gpg4win.org/

Linux: (molemmat voivat olla asennettu, mutta toisellakin pärjää) gnupg (v.1.4 standalone, ei patentoituja algoritmeja) gnupg2 (modulaarinen, IDEA-algoritmi)

osallistujat

Ilmoittautuneita on jo näin monta tukkimiestä ja -naista

II

HUOM

Koska ilta on suunnattu ensisijaisesti ennestään PGP:tä käyttämättömille henkilöille, aikaa ei todennäköisesti riitä keysigning partyyn, joka kuitenkin järjestetään myöhemmin tai tarvittaessa.