Áttekintés a GPG/PGP-ről

Mohácsi János
NIIF Intézet

2007.10.07.

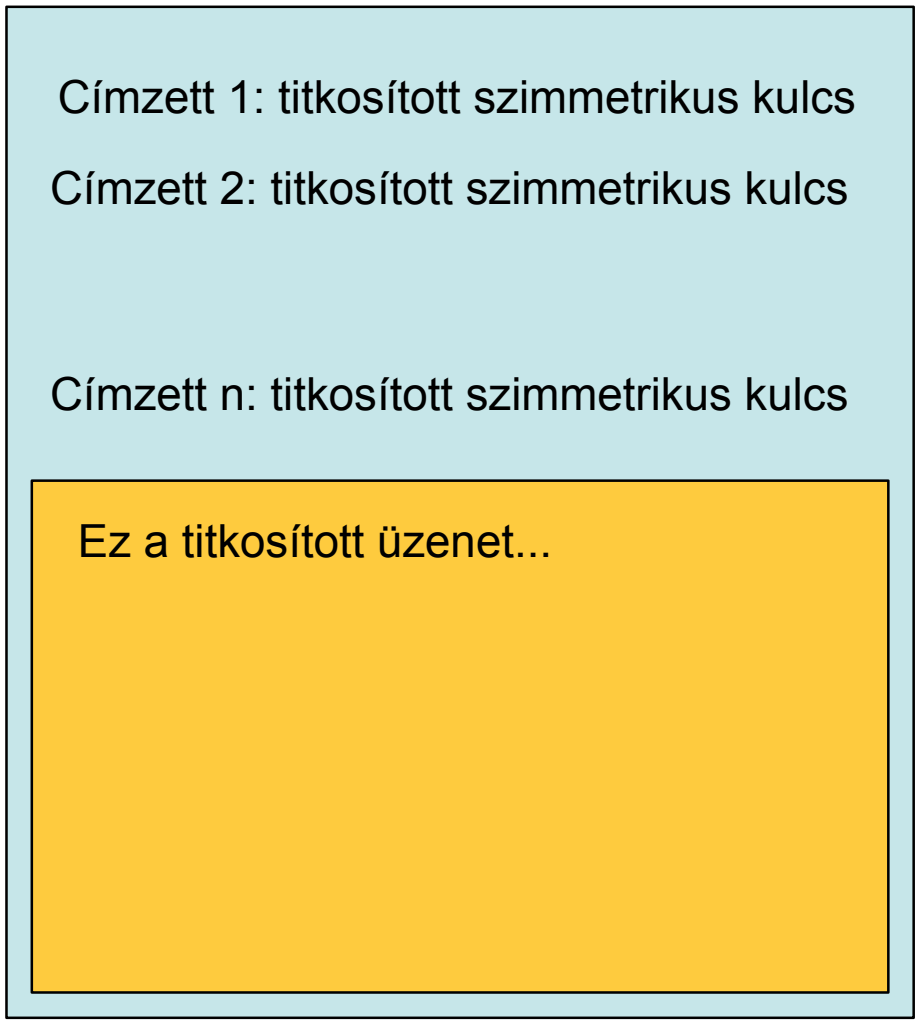
Tartalomjegyzék

- Bevezetés
- Technikai háttér
- Web of trust
- GPG/PGP használata
- Kulcs aláírási est

Történelem

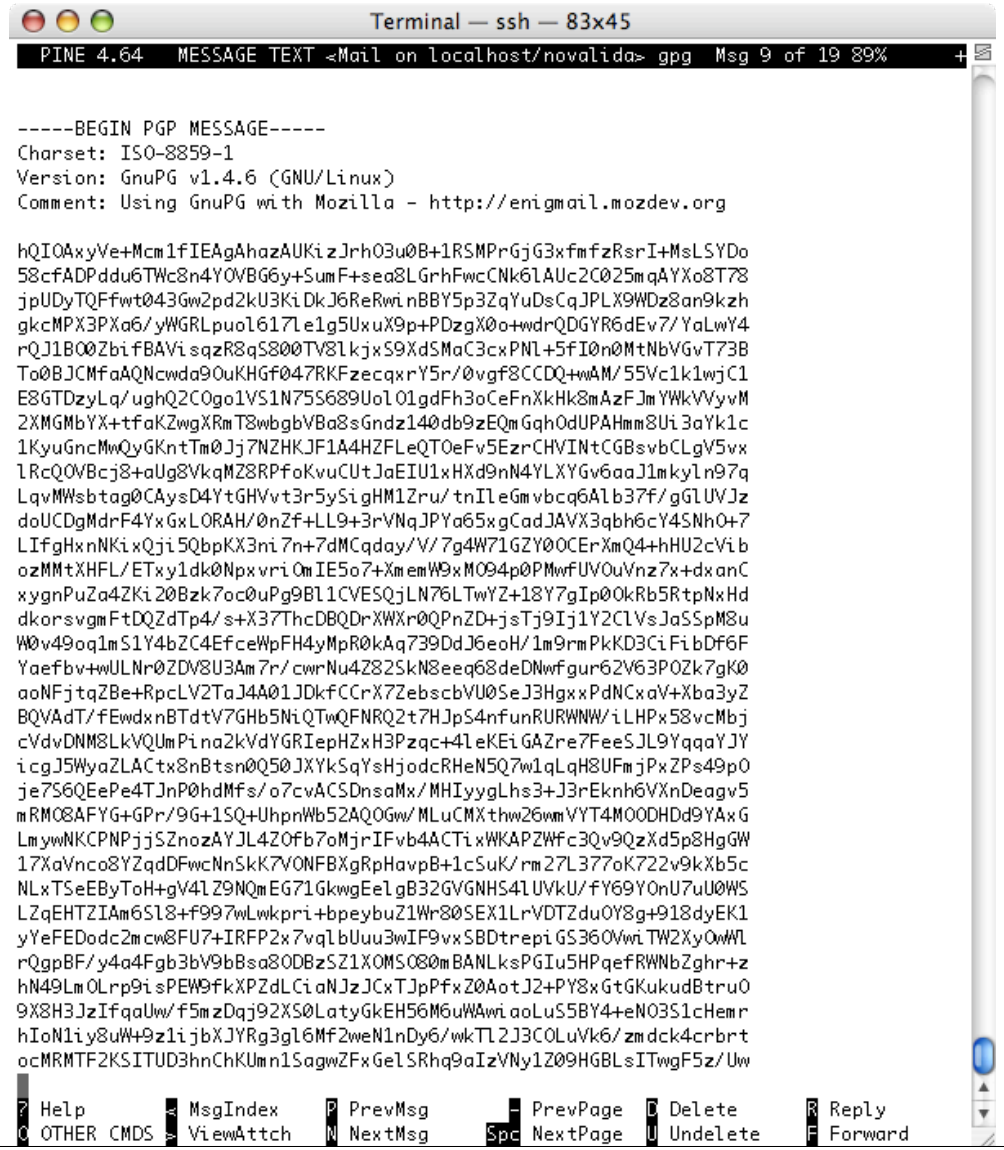
- 1991: Phil Zimmermann megírja a PGP-t mint public domain szoftvert - export tilalom
  - export elkerülés - csak elektronikusan tilos exportálni - a könyvet ki lehet vinni
- 1996: a büntetés felfüggesztése - Phil megalapítja PGP Inc.-et
- 1997: Network Associates megvásárolja PGP Inc.-et
  - 2 változat: PGP(US) és PGPi (nemzetközi)
  - jogi problémák az IDEA algoritmussal
- Gnupg 1.x (old), gnupg 2.x (current) (GNU privacy guard)
  - ElGamal (aláírás és titkosítás), DSA, RSA,
  - AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 and TIGER
  - IDEA pluginnel

Működés

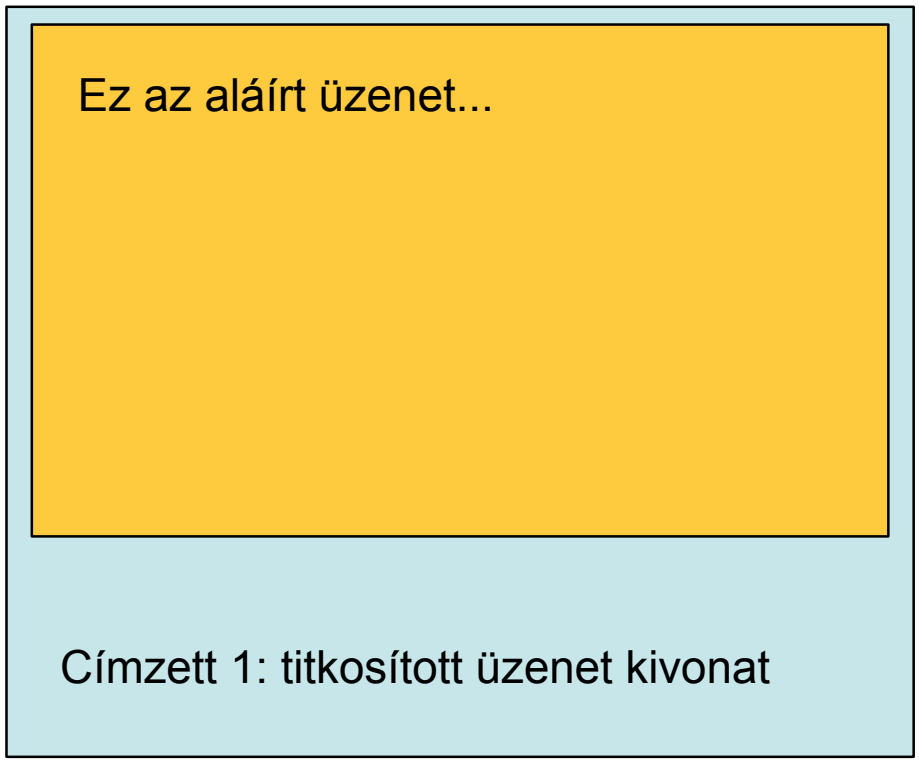


- Titkosítás:
  - A publikus kulcsa: P_A
  - GPG generál egy véletlen kulcsot k
  - tikosított üzenet elküldése [$SIM_k(T)$,$P_A(k)$]
- Titkosított levél olvasás:
  - fogadás [$SIM_k(T)$,$P_A(k)$]
  - A session kulcs kinyerése: $k=S_A(P_A(k))$;
  - titkos üzenet kibontás: $T=SIM_k(SIM_k(T))$

Működés /2

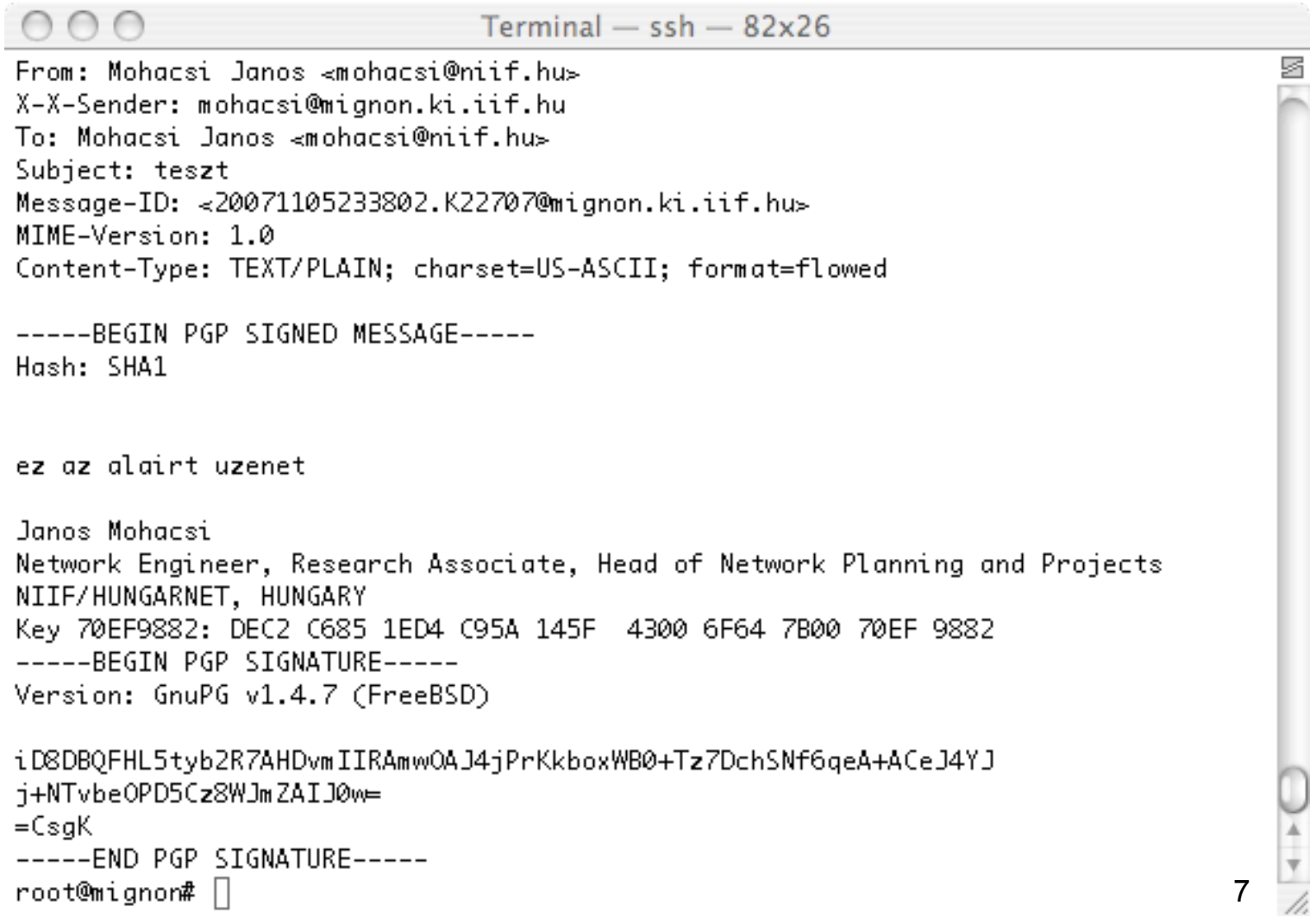

Terminal — ssh — 83x45
PINE 4.64 MESSAGE TEXT <Mail on localhost/novalida> gpg Msg 9 of 19 89%
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.4.6 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org
hQIOAxyVe+Mcm1fIEAgAhazAUKizJrhO3u0B+1RSMPrGjG3xfmfzRsrI+MsLSYDo
58cfADPddu6TWc8n4YOVBG6y+SumF+sea8LGrhFwcCNk6lAUc2C025mqAYXo8T78
jpUDyTQFfwt043Gw2pd2kU3KiDkJ6ReRwinBBY5p3ZqYuDsCqJPLX9WDz8an9kzh
gkcMPX3PXa6/yWGRLpuol617le1g5UxuX9p+PDzgX0o+wdrQDGYR6dEv7/YaLwY4
rQJ1BO0ZbifBAVisqzR8qS800TV8lkjxS9XdSMaC3cxPNl+5fI0n0MtNbVGvT73B
To0BJCMfaAQNcwda9OuKHGf047RKFzecqxrY5r/0vgf8CCDQ+wAM/55Vc1k1wjC1
E8GTDzyLq/ughQ2COgo1VS1N75S689UolO1gdFh3oCeFnXkHk8mAzFJmYWkVVyvM
2XMGMbYX+tfaKZwgXRmT8wbgbVBa8sGndz140db9zEQmGqhOdUPAHmm8Ui3aYk1c
1KyuGncMwQyGKntTm0Jj7NZHKJF1A4HZFLeQTOeFv5EzrCHVINtCGBsvbCLgV5vx
lRcQOVBcj8+aUg8VkqMZ8RPfoKvuCUtJaEIU1xHXd9nN4YLXYGv6aaJ1mkyln97q
LqvMWsbtag0CAysD4YtGHVvt3r5ySigHM1Zru/tnIleGmvbcq6Alb37f/gGlUVJz
doUCDgMdrF4YxGxLORAH/0nZf+LL9+3rVNqJPYa65xgCadJAVX3qbh6cY4SNhO+7
LIfgHxnNKixQji5QbpKX3ni7n+7dMCqday/V/7g4W71GZY0OCErXmQ4+hHU2cVib
ozMMtXHFL/ETxy1dk0NpxvriOmIE5o7+XmemW9xMO94p0PMwfUVOuVnz7x+dxanC
xygnPuZa4ZKi20Bzk7oc0uPg9Bl1CVESQjLN76LTwYZ+18Y7gIp0OkRb5RtpNxHd
dkorsvgmFtDQZdTp4/s+X37ThcDBQDrXWXr0QPnZD+jsTj9Ij1Y2ClVsJaSSpM8u
W0v49oq1mS1Y4bZC4EfceWpFH4yMpR0kAq739DdJ6eoH/1m9rmPkKD3CiFibDf6F
Yaefbv+wULNr0ZDV8U3Am7r/cwrNu4Z82SkN8eeq68deDNwfgur62V63POZk7gK0
aoNFjtqZBe+RpcLV2TaJ4A01JDkfCCrX7ZebscbVU0SeJ3HgxxPdNCxaV+Xba3yZ
BQVAdT/fEwdxnBTdtV7GHb5NiQTwQFNRQ2t7HJpS4nfunRURWNW/iLHPx58vcMbj
cVdvDNM8LkVQUmPina2kVdYGRIepHZxH3Pzqc+4leKEiGAZre7FeeSJL9YqqaYJY
icgJ5WyaZLACtx8nBtsn0Q50JXYkSqYsHjodcRHeN5Q7w1qLqH8UFmjPxZPs49pO
je7S6QEePe4TJnP0hdMfs/o7cvACSDnsaMx/MHIyygLhs3+J3rEknh6VXnDeagv5
mRMC8AFYG+GPr/9G+1SQ+UhpnWb52AQOGw/MLuCMXthw26wmVYT4MOODHDd9YAxG
LmywwNKCPNPjjSZnozAYJL4ZOfb7oMjrIFvb4ACTixWKAPZWfc3Qv9QzXd5p8HgGW
17XaVnco8YZqdDFwcNnSkK7VONFBXgRpHavpB+1cSuK/rm27L377oK722v9kXb5c
NLxTSeEByToH+gV4lZ9NQmEG71GkwgEelgB32GVGNHS4lUVkU/fY69YOnU7uU0WS
LZqEHTZIAm6Sl8+f997wLwkpri+bpeybuZ1Wr80SEX1LrVDTZduOY8g+918dyEK1
yYeFEDodc2mcw8FU7+IRFP2x7vqlbUuu3wIF9vxSBDtrepiGS36OVwiTW2XyOwWl
rQgpBF/y4a4Fgb3bV9bBsa8ODBzSZ1XOMSO80mBANLksPGIu5HPqefRWNbZghr+z
hN49LmOLrp9isPEW9fkXPZdLCiaNJzJCxTJpPfxZ0AotJ2+PY8xGtGKukudBtruO
9X8H3JzIfqaUw/f5mzDqj92XS0LatyGkEH56M6uWAwiaoLuS5BY4+eNO3S1cHemr
hIoN1iy8uW+9z1ijbXJYRg3gl6Mf2weN1nDy6/wkTl2J3COLuVk6/zmdck4crbrt
ocMRMTF2KSITUD3hnChKUmn1SagwZFxGelSRhq9aIzVNy1Z09HGBLsITwgF5z/Uw
? Help < MsgIndex P PrevMsg - PrevPage D Delete R Reply
O OTHER CMDS > ViewAttch N NextMsg Spc NextPage U Undelete F Forward

Működés /3



- Aláírás
  - Üzenet kivonat generálás: MD(T)
  - A elküldi a következőt : $[T,S_A(MD(T))]$
- Aláírás ellenőrzés
  - Fogadás: $[T,S_A(MD(T))]$
  - kibontáa: $DD=P_A(S_A(MD(T)))$
  - Üzenet kivonat: MD(T)
  - Összehasonlítás: MD(T) és DD

Működés/4

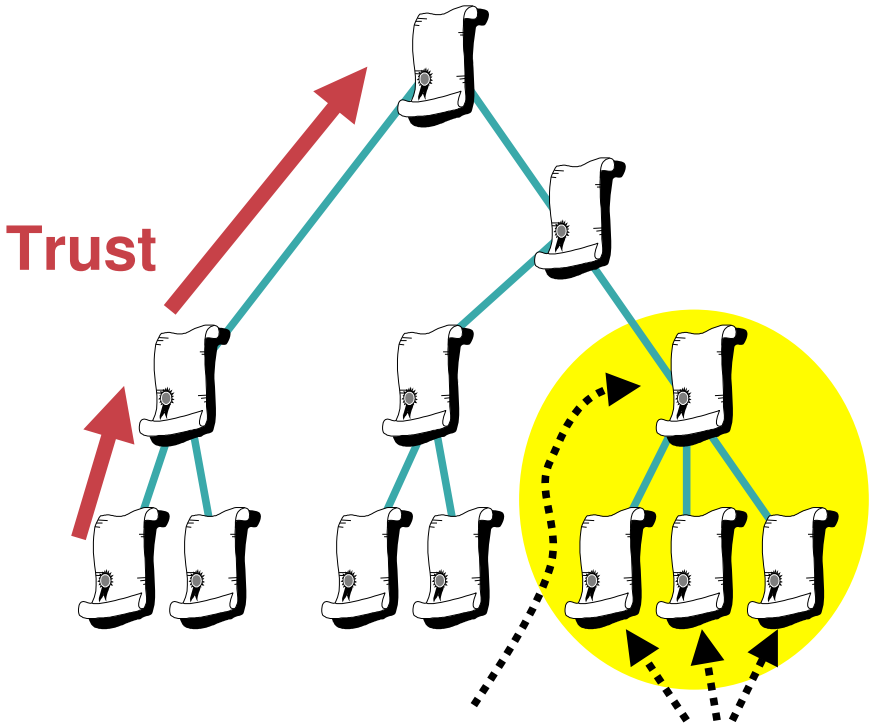

Terminal — ssh — 82x26
From: Mohacsi Janos <mohacsi@niif.hu>
X-X-Sender: mohacsi@mignon.ki.iif.hu
To: Mohacsi Janos <mohacsi@niif.hu>
Subject: teszt
Message-ID: <20071105233802.K22707@mignon.ki.iif.hu>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
ez az alairt uzenet
Janos Mohacsi
Network Engineer, Research Associate, Head of Network Planning and Projects
NIIF/HUNGARNET, HUNGARY
Key 70EF9882: DEC2 C685 1ED4 C95A 145F 4300 6F64 7B00 70EF 9882
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.7 (FreeBSD)
iD8DBQFHL5tyb2R7AHDvmIIRAmwOAJ4jPrKkboxWB0+Tz7DchSNf6qeA+ACeJ4YJ
j+NTvbeOPD5Cz8WJmZAIJ0w=
=CsgK
-----END PGP SIGNATURE-----
root@mignon#

PGP vs X.509

- X.509 C A -t igényel, PGP-ben lehetőség van a kulcsok kölcsönös tanusítására
- X.509 csak egyetlen ID-t tesz lehetővé egy certificate-hez. PGP sokat
- X.509 csak egy aláírást tesz lehetővé, PGP sokat

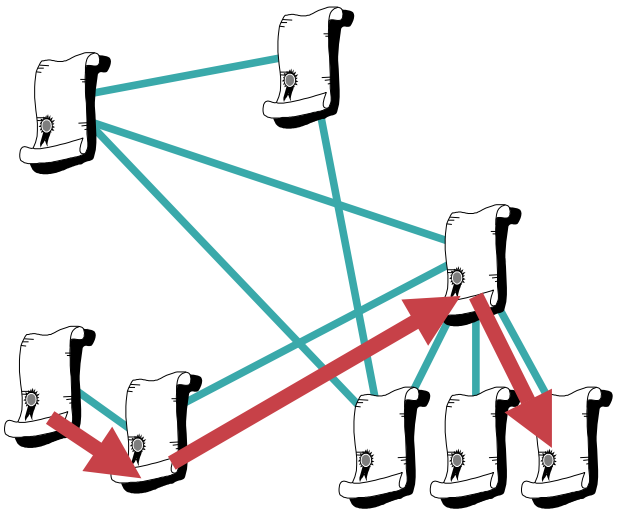
Bizalmi modellek

Hierarchical



Example: CA and routers

Web of Trust

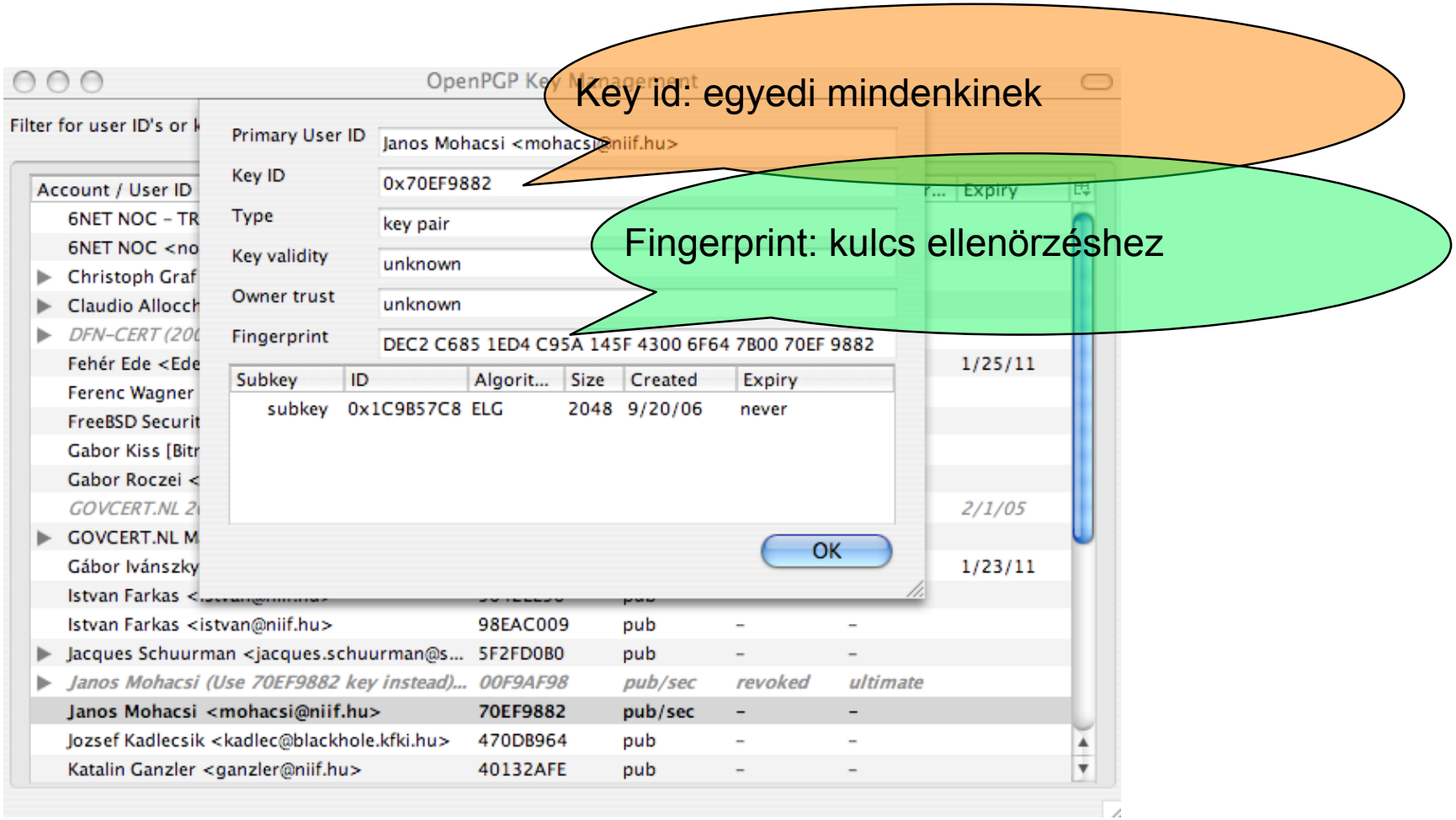


Example: PGP

Problémák a web of trust-al

- Nem hierarchikus
- Flexibilis - ott lehet építeni a bizalmi viszonyokat ahol szükséges - de ott kell is
- De milyen hosszú lehet a bizalmi lánc
- PGP:
  - Validitás: kulcs helyes
    - Valid, marginally valid , invalid
  - Bizalom: Megbízok egy adott személyben, hogy másokat a bizalmi hálóba bevezessen
    - Full trust: Megbízom azokban a kulcsokban amellyeket ez a kulcs aláírt
    - Marginal trust: Megbízom azokban a kulcsokban amelyeket legalább 2 marginally trusted kulcs aláírt
    - No trust: Nem bízom azokban a kulcsokban amelyeket ez a kulcs aláírt

Kulcs menedzsment



Kulcspár létrehozás

- Kulcspár generálás: RSA vagy DH/DSS (vagy DSA/El-Gamal)
- Kulcshosz: Legalább1024 bit; javasolt méretek: DH >2048, DSS >1024
- ID : Nev <your.name@domain.com>
- Opcionális: Lejárat

Kulcspár létrehozás /2

- Az egész biztonság a jelmondaton (passphrase) múlik! - elég erősnek kell lennie
- Nem lehet visszanyerni! Nem célszerű elfelejteni
- Ha mégis elfelejtjük:
  - Nem tudjuk visszavonni a kulcsot (a titkoskulcshoz hozzá kell tudni férni ;-)
  - Nem tudunk titkosított üzenetet fogadni, titkosított fájlokat visszafejteni és aláírni

Kulcsszerver

- Tulajdonképpen egy directory - kulcstár
- Csak egy tároló - semmilyen bizalmi funkciója nincsen
- Elvileg minden kulcs szerver szinkronizál
- Tipikus működések
  - receive keys
  - refresh keys
  - send key

Kulcs visszavonás

- Visszavonási kulcs generálás - a privát kulcs segítségével
- A visszavonási kulcs publikálása → A kulcsot megöltük... visszavonásra került!

GPG kulcsaláírási est

- Cél: GPG/PGP kulcsok alkalmazásának támogatása
- Helyszín
  - Mátrafüredi Akadémiai Üdülő és Malom fogadó 3232 Mátrafüred, Akadémia u. 1-3.
- Időpont
  - 2007. november 7. 17:20 - 18:20 CET
- Szükséges dolgok
  - Fizikai jelenlét
  - Érvényes fényképes hatósági igazolvány (pl. Személyi igazolvány, új fajta jogosítvány, útlevél stb)
  - GPG/PGP kulcs azonosítója, mérete, típusa, hexadecimális ujjlenyomata (gpg@niif.hu)
  - Toll/ceruza, vagy valamilyen író eszköz
  - Nincs szükség számítógépre

GPG kulcsaláírási est/2

- Lista kiosztás
- Kulcsaláírási esetén a kulcs tulajdonosa magával hozott papírról felolvassa a publikus kulcs azonosítóját, méretét, típusát és ujjlenyomatát.
- Ha a felolvasott információ és a nyomtatott listás információ megegyezik a résztvevők 1 jelet tehetnek az adott kulcshoz.
- Mindenki ellenőrzi mindenki személy azonosságát.
- Pontosan akkor még egy jelet tehetnek a részvevők az adott kulcshoz, ha meggyőződtek, arról hogy az aki azt állítja magáról, hogy xy az valóban xy és valóban az övé a publikus kulcs.
- Otthon, ha ellenőriztük, hogy a listán szereplő azon kulcsok, melyek mellett 2 jel van, megegyeznek a publikus kulcsszerveren tárólt kulccsal, akkor aláírhatjuk. Csak akkor írjuk alá a kulcsot, ha 2 jel van mellette!
- Updateljük a kulcsszerveren az általunk aláírt kulcsokat.

Kérdés

Bővebb információ

http://www.hbone.hu/Workshop2007/hbone-gpg-keysigning.html

?