Jabber i GnuPG
una comunicacio distribuida, instantania i segura

Que es Jabber

- **Jabber és un protocol XML obert per a l'intercanvi de missatges i informació de presència en temps real entre dos punts qualssevol de la Internet.**
- **Es una plataforma de missatgeria instantània (MI) asíncrona (els msg no entregats s'emmagatzemen al servidor) i extensible.**

Caracteristiques de Jabber

- **Obert: el protocol Jabber és lliure, obert, públic i fàcilment comprensible, i existeixen múltiples implementacions de servidors, clients i biblioteques de programació.**
- **Extensible: utilitzant la potència de l'XML és possible ampliar el protocol Jabber per realitzar noves funcions. A fi de mantenir la compatibilitat, les extensions comunes són gestionades per la Jabber Software Foundation.**

Caracteristiques Jabber II

- **Descentralitzat: qualsevol pot instal·lar i administrar el seu servidor Jabber, de manera que els individus i les organitzacions tenen un control total sobre el seu sistema de missatgeria instantània.**
- **Segur: Qualsevol servidor Jabber pot estar aïllat de la xarxa Jabber pública, moltes implementacions fan servir SSL per a la comunicació entre client i servidor i molts clients admeten xifratge PGP/GPG per a la comunicació d'usuari a usuari;**

Que es l'XML?

- **XML es l'acrònim anglès d'eXtensible Markup Language**

- **Havia de ser un substitut de l'HTML, ja que té una manca de funcionalitats, i és una mica pobre per les necessitats actuals.**

- **S'assembla a l'HTML en l'us d'etiquetes per a delimitar els elements d'un document. Per contra XML defineix les etiquetes en funció del tipus de dades que esta describint i no de l'aparença final que tendran en pantalla o a la copia impresa, a mes permet definir noves etiquetes i ampliar les existents.**

Clients i Servidors

CLIENTS

- **PSI (http://psi.affinix.com)**
- **Exodus**
- **Gabber**
- **...**

SERVIDORS

- **Antepo OPN**
- **Ejabberd**
- **Jabber XCP**
- **jabberd 1.x**
- **...**

Per a mes informacions podeu consultar el google, o www.jabber.org

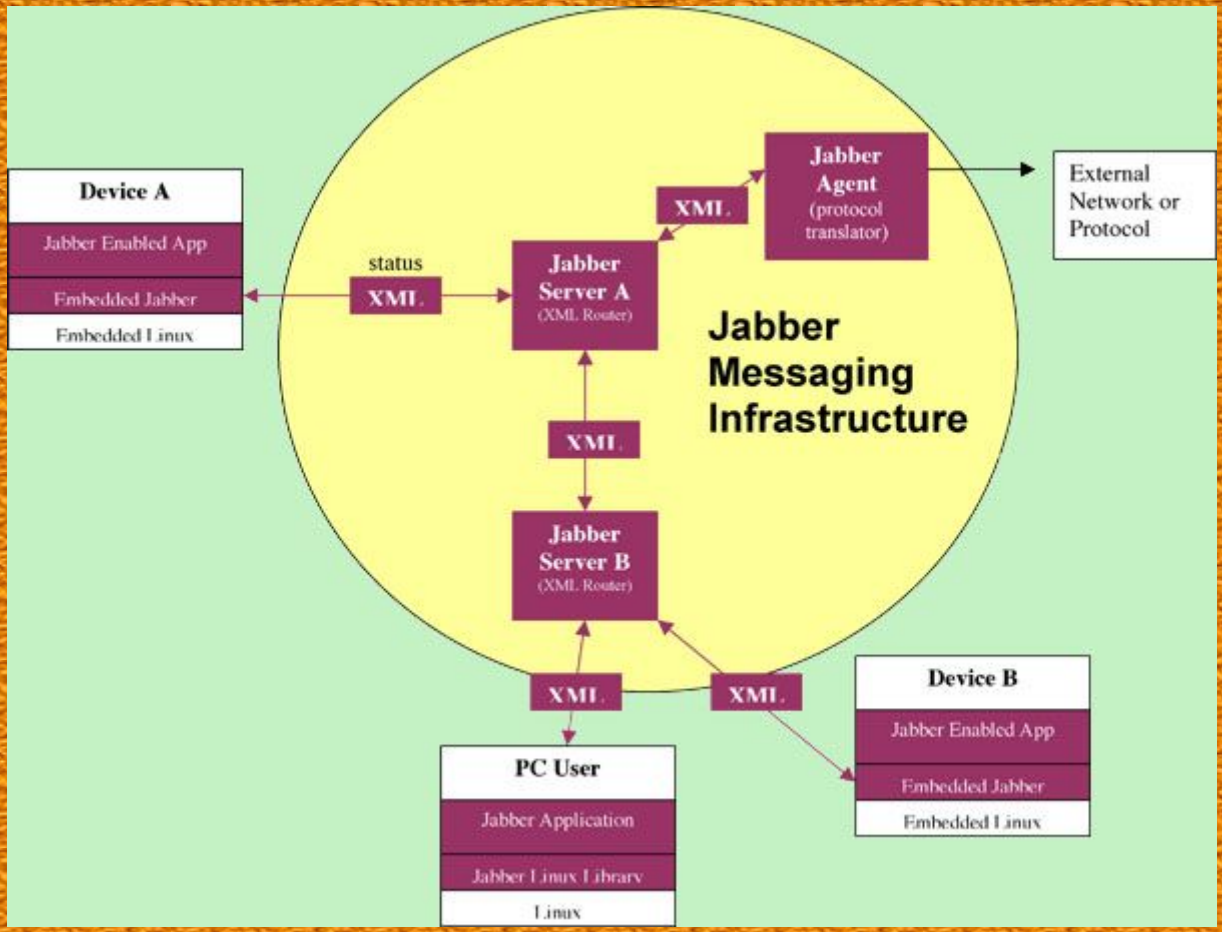
Servidors

- **Com instal·lar un servidor jabber "de serie".**

  $ apt-get install jabber

  si volem que sigui públic ho haurem de configurar a part (/etc/jabber/jabber.xml)
- **Podem instal·lar l'SSL per a logins segurs**
- **Les passarel·les serveixen per a unir tots els serveis d'IM en el client de Jabber. El MSN-Transport permet de tenir els contactes de msn junt amb els de jabber.**

La xarxa Jabber



PGP

- **Pretty Good Privacy**
- **Creat per Phil Zimmerman cap al 1990**
- **Simplica el procés de xifrar/desxifrar**
- **Xifra amb clau simètrica aleatòria que adjunta xifrada amb una altra clau asimètrica.**

PGP(2)

- **Phil Zimmerman va tenir problemes**
  - **Amb el govern dels USA**
  - **amb RSA Data Security inc**
- **La idea va ser comprada i recomprada fins avui.**
- **PGP Corporation ofereix una versió gratuita per a usos no lucratius.**

OpenPGP

- **És un estandard de xifrat basat en PGP**
  - **Creat per la IETF**
  - **RFC 2440**
- **És no-propietari**
  - **Qualsevol el pot implementar sense pagar cap llicència.**
- **Actualment s'ha convertit en el sistema de xifrat (sobretot d'emails) més usat**

GnuPG

- És una implentació de OpenPGP
- Utilitza algorismes no patentats
  - DSA/ElGamal (RSA esta patentat)
- Sota llicència GNU
  - Es distribueix amb el codi font
  - Existeix per a múltiples plataformes
    - Variants Unix
    - Windows
    - PocketPC
    - .....

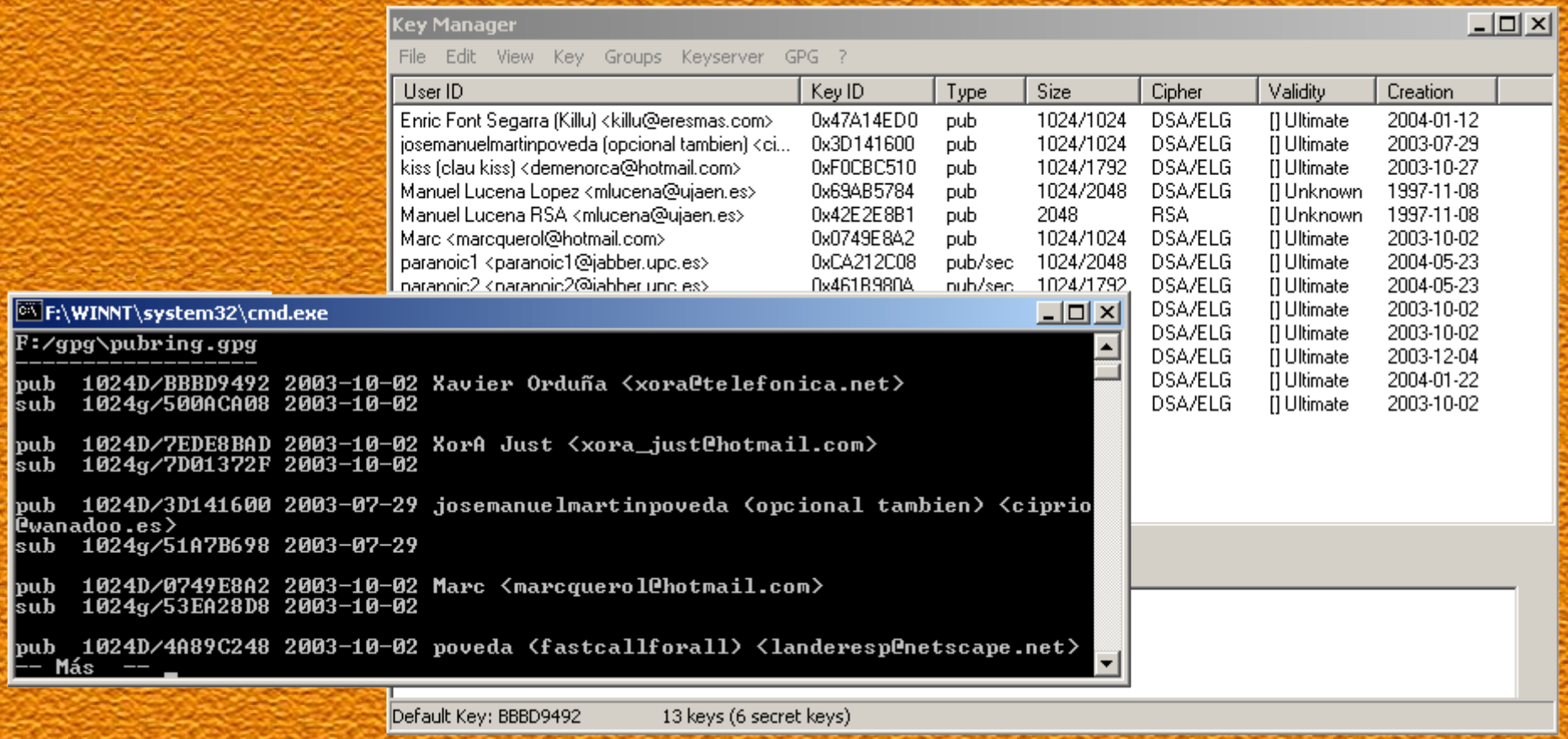
GnuPG(2)

- **Un sol executable.**
- **Sense instalació adicional.**
- **S'utilitza a través de línia de comandes**
  - **Molt flexible.**
  - **Pot ser usat desde qualsevol llenguatge:**
    - **Scripts PHP, Perl, bash...**
    - **Crides fork().**
  - **Inicialment pot semblar dificil d'utilitzar.**

FrontEnds per a GPG

- **Existeixen frontends i plugins**
  - **Interactuen de forma transparent amb l'executable**
  - **Manegadors de claus:**
    - **WinPT, GPA, Kgpg....**
  - **Xifrat/desxifrat de correus:**
    - **Enigmail, EudoraGPG, GPGOE, ...**
- **Per a qualsevol plataforma**
- **Posen la criptografia a l'abast de tots**

Frontends (2)


Key Manager
File Edit View Key Groups Keyserver GPG ?
User ID | Key ID | Type | Size | Cipher | Validity | Creation
Enric Font Segarra (Killu) <killu@eresmas.com> 0x47A14ED0 pub 1024/1024 DSA/ELG [] Ultimate 2004-01-12
josemanuelmartinpoveda (opcional tambien) <ci... 0x3D141600 pub 1024/1024 DSA/ELG [] Ultimate 2003-07-29
kiss (clau kiss) <demenorca@hotmail.com> 0xF0CBC510 pub 1024/1792 DSA/ELG [] Ultimate 2003-10-27
Manuel Lucena Lopez <mlucena@ujaen.es> 0x69AB5784 pub 1024/2048 DSA/ELG [] Unknown 1997-11-08
Manuel Lucena RSA <mlucena@ujaen.es> 0x42E2E8B1 pub 2048 RSA [] Unknown 1997-11-08
Marc <marcquerol@hotmail.com> 0x0749E8A2 pub 1024/1024 DSA/ELG [] Ultimate 2003-10-02
paranoic1 <paranoic1@jabber.upc.es> 0xCA212C08 pub/sec 1024/2048 DSA/ELG [] Ultimate 2004-05-23
DSA/ELG [] Ultimate 2004-05-23
DSA/ELG [] Ultimate 2003-10-02
DSA/ELG [] Ultimate 2003-10-02
DSA/ELG [] Ultimate 2003-12-04
DSA/ELG [] Ultimate 2004-01-22
DSA/ELG [] Ultimate 2003-10-02
Default Key: BBBD9492 13 keys (6 secret keys)
F:\WINNT\system32\cmd.exe
F:/gpg\pubring.gpg
pub 1024D/BBBD9492 2003-10-02 Xavier Orduña <xora@telefonica.net>
sub 1024g/500ACA08 2003-10-02
pub 1024D/7EDE8BAD 2003-10-02 XorA Just <xora_just@hotmail.com>
sub 1024g/7D01372F 2003-10-02
pub 1024D/3D141600 2003-07-29 josemanuelmartinpoveda (opcional tambien) <ciprio
@wanadoo.es>
sub 1024g/51A7B698 2003-07-29
pub 1024D/0749E8A2 2003-10-02 Marc <marcquerol@hotmail.com>
sub 1024g/53EA28D8 2003-10-02
pub 1024D/4A89C248 2003-10-02 poveda (fastcallforall) <landeresp@netscape.net>
-- Más --

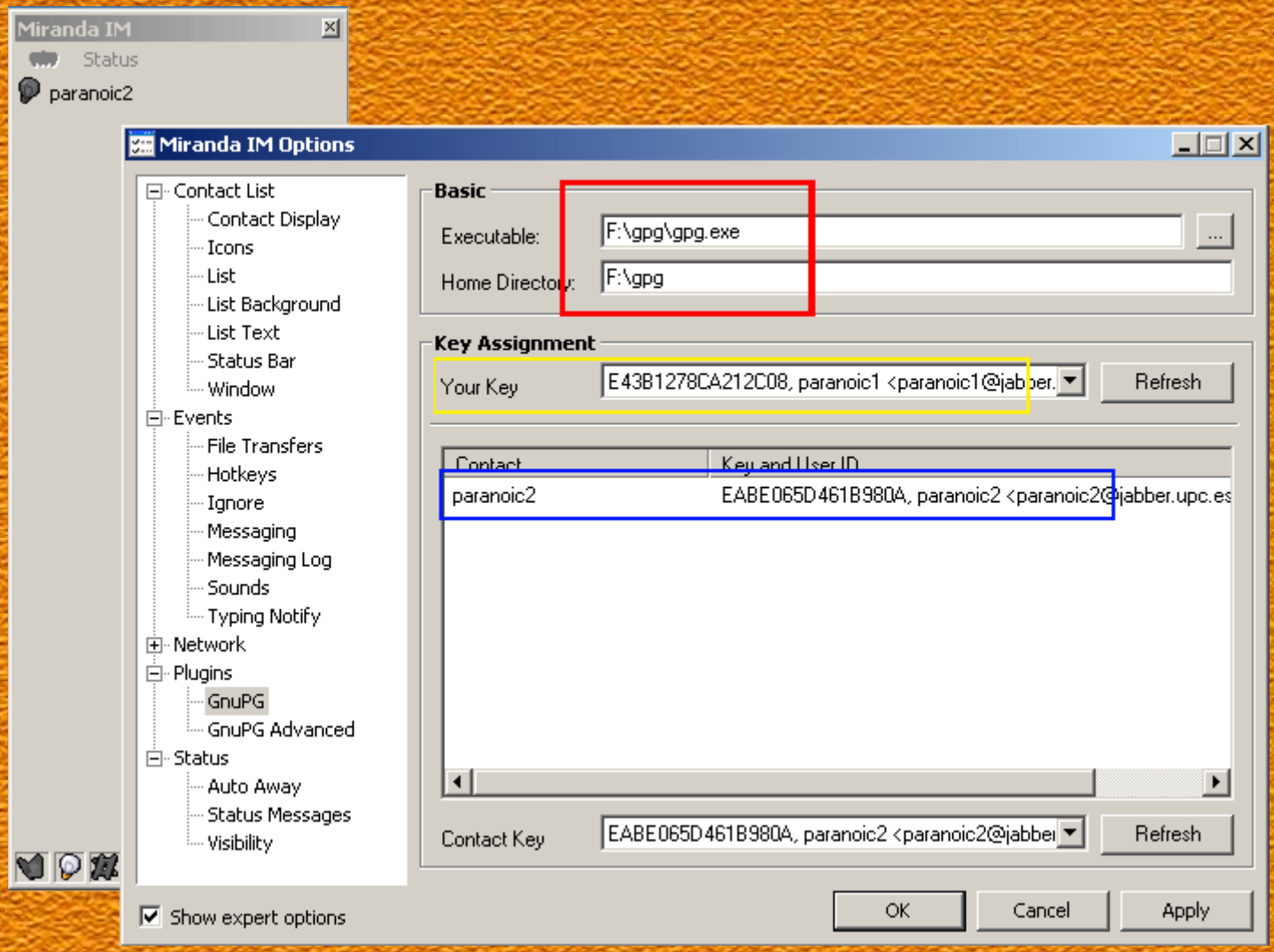
Missatgeria Instantània + GnuPG

- **Hi ha diversos clients de IM que usen GPG per a xifrar converses**
  - **Miranda**
  - **Gabber**
  - **Psi**
  - **Tkabber**

Miranda

- **Client Multiprotocol**
- **Xifra el missatge i l'envia directament usant OpenPGP**
  - **No és estandard i només funciona amb altres Miranda**
  - **Molt ineficient**
- **Disponible només per a Windows**
- **http://miranda-im.org**

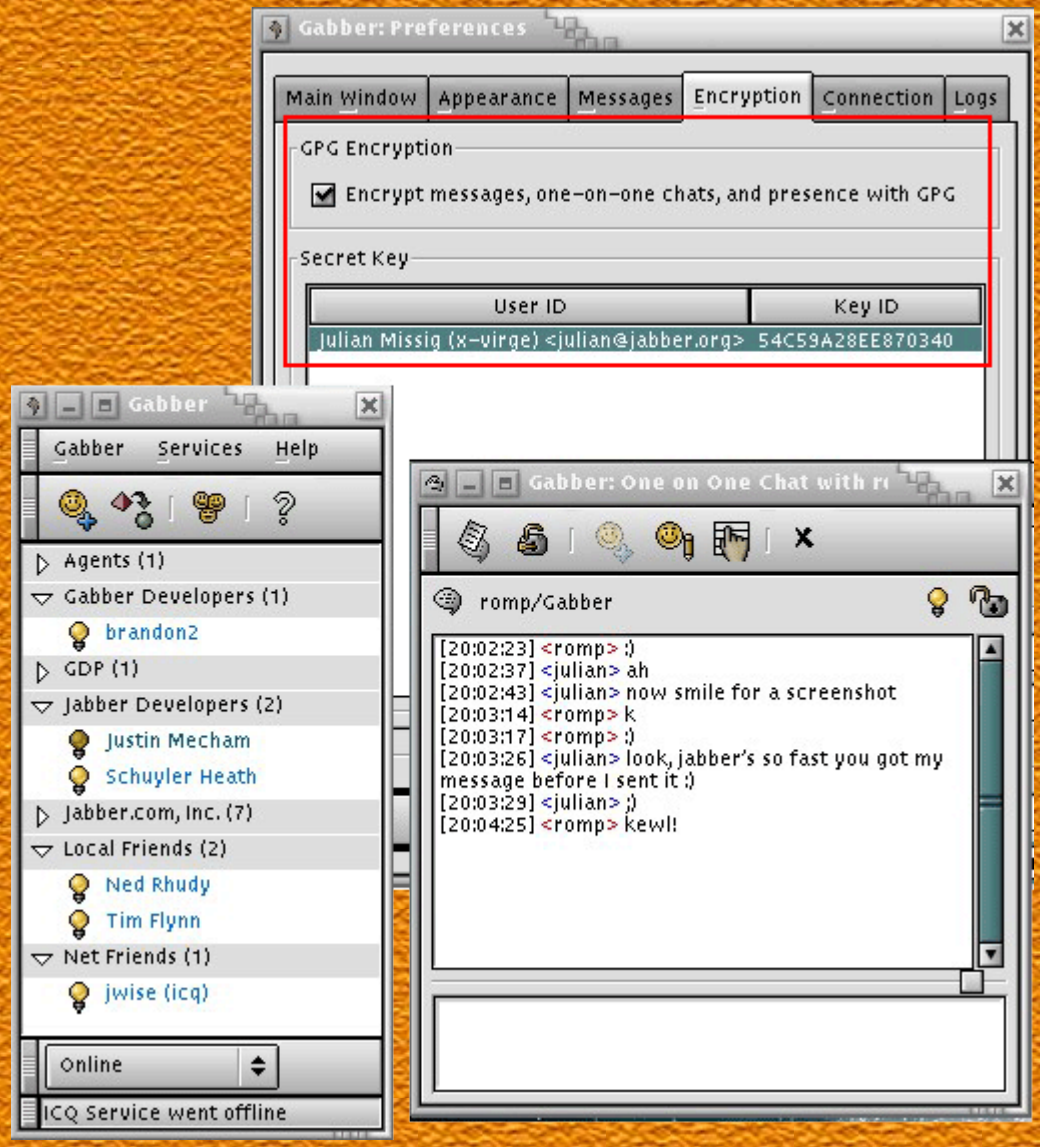
Miranda(2)


Miranda IM
Status
paranoic2
Miranda IM Options
Contact List
Contact Display
Icons
List
List Background
List Text
Status Bar
Window
Events
File Transfers
Hotkeys
Ignore
Messaging
Messaging Log
Sounds
Typing Notify
Network
Plugins
GnuPG
GnuPG Advanced
Status
Auto Away
Status Messages
Visibility
Basic
Executable:
F:\gpg\gpg.exe
Home Directory:
F:\gpg
Key Assignment
Your Key
E43B1278CA212C08, paranoic1 <paranoic1@jabber.
Refresh
Contact
Key and User ID
paranoic2
EABE065D461B980A, paranoic2 <paranoic2@jabber.upc.es
Contact Key
EABE065D461B980A, paranoic2 <paranoic2@jabber
Refresh
Show expert options
OK
Cancel
Apply

Gabber

- **Client Jabber**
  - **Pot utilitzar altres xarxes (Msn, ICQ, IRC) a través de passarel·les**
- **El OpenPGP està integrat al protocol jabber**
  - **Eficient**
  - **Compatible amb clients diferents**
- **Només disponible per a Linux**
- **http://gabber.sourceforge.net**

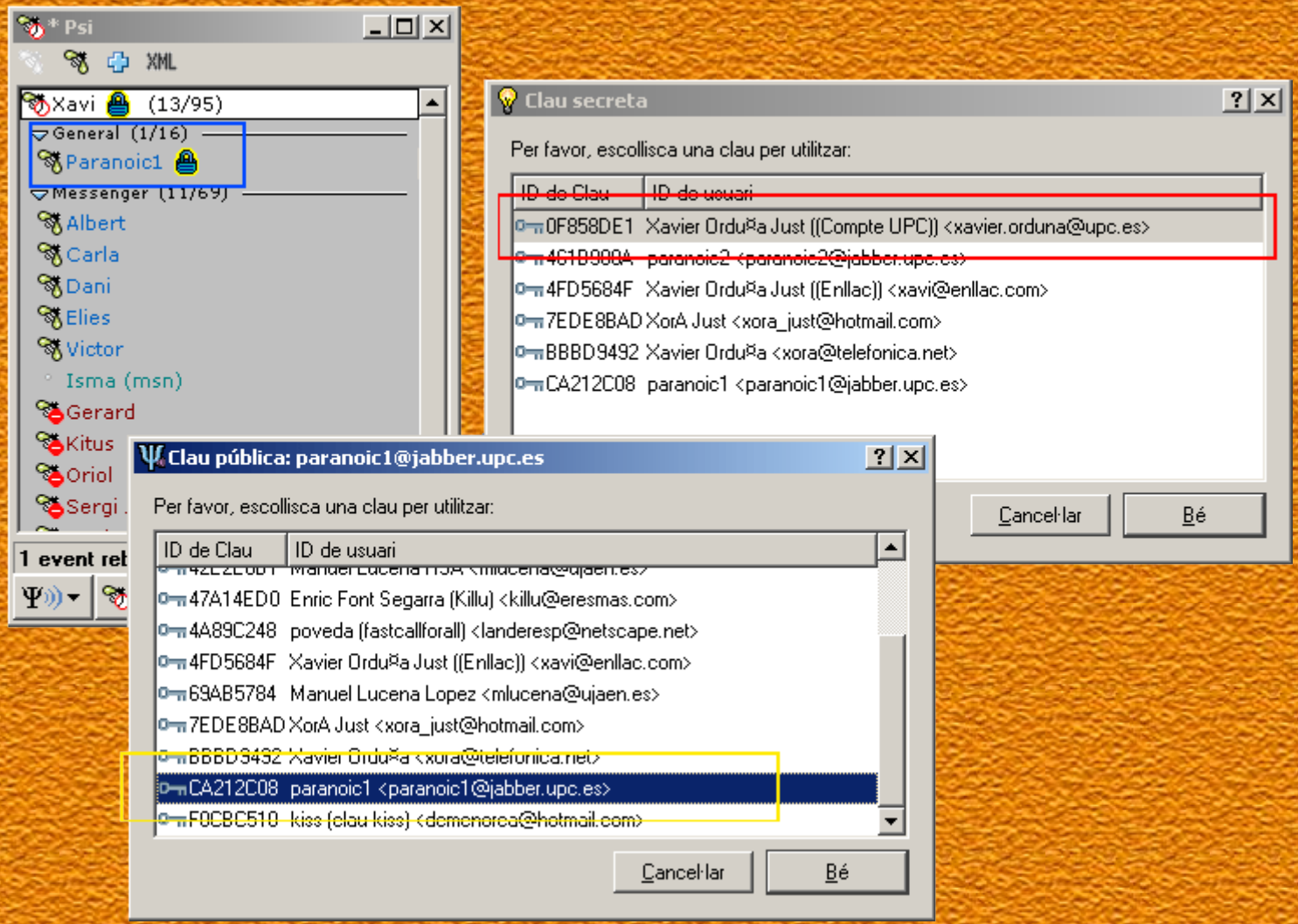
Gabber(2)


Gabber: Preferences
Main Window
Appearance
Messages
Encryption
Connection
Logs
GPG Encryption
Encrypt messages, one-on-one chats, and presence with GPG
Secret Key
User ID
Key ID
Julian Missig (x-virge) <julian@jabber.org> 54C59A28EE870340
Gabber
Gabber
Services
Help
Agents (1)
Gabber Developers (1)
brandon2
GDP (1)
Jabber Developers (2)
Justin Mecham
Schuyler Heath
Jabber.com, Inc. (7)
Local Friends (2)
Ned Rhudy
Tim Flynn
Net Friends (1)
jwise (icq)
Online
ICQ Service went offline
Gabber: One on One Chat with r
romp/Gabber
[20:02:23] <romp> :)
[20:02:37] <julian> ah
[20:02:43] <julian> now smile for a screenshot
[20:03:14] <romp> k
[20:03:17] <romp> :)
[20:03:26] <julian> look, jabber's so fast you got my message before I sent it :)
[20:03:29] <julian> ;)
[20:04:25] <romp> kewl!

Psi

- **Basat en QT**
  - **Disponible per a multiples plataformes**
    - **Linux, Windows, MacOS**
- **OpenPGP integrat al protocol**
- **No usa totes les capacitats de Jabber**
- **AutoDetecta l'existència de GPG**
- **http://psi.affinix.com**

Psi(2)

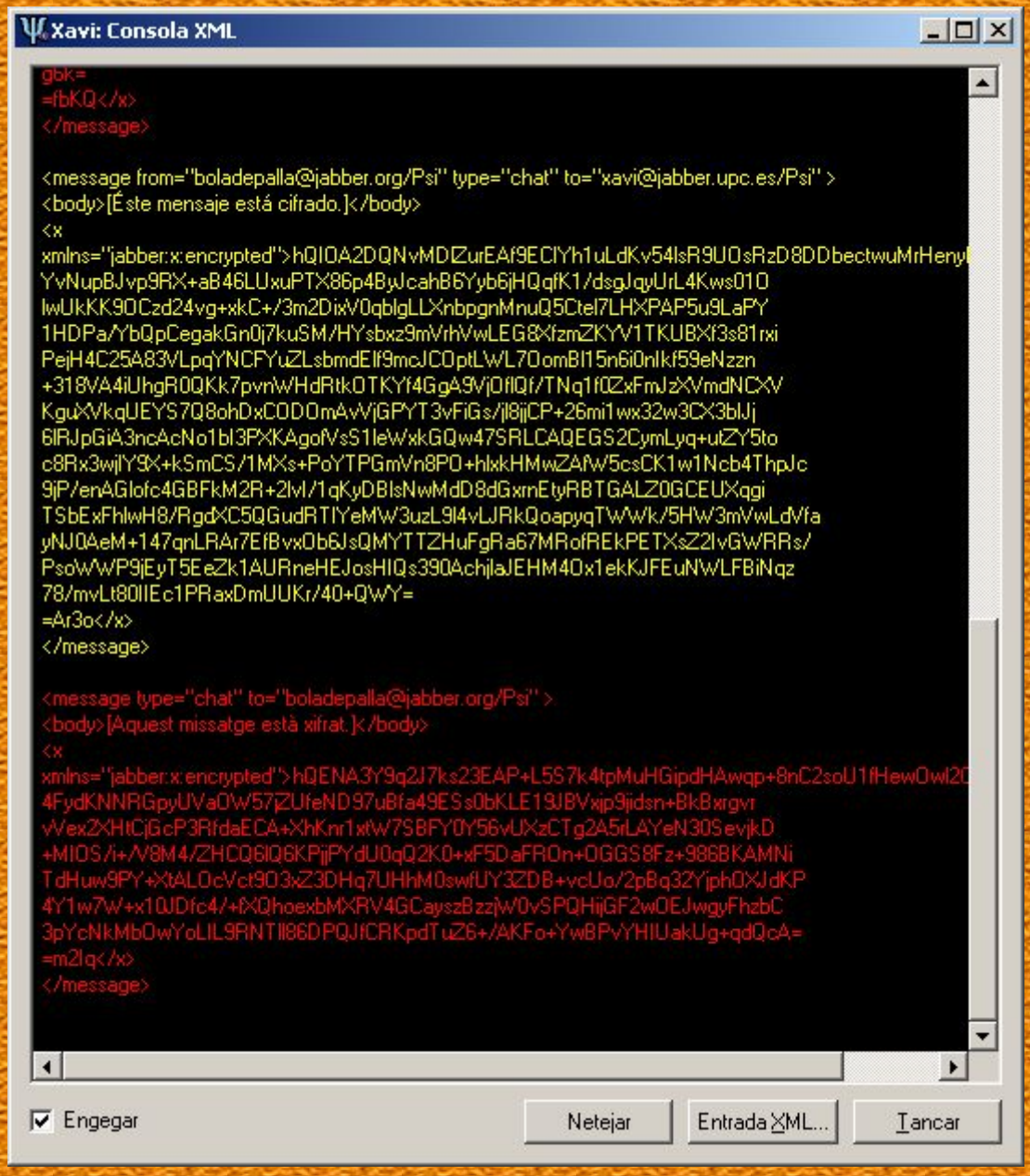

* Psi
XML
Xavi (13/95)
General (1/16)
Paranoic1
Messenger (11/69)
Albert
Carla
Dani
Elies
Victor
Isma (msn)
Gerard
Kitus
Oriol
Sergi
1 event ret
Clau secreta
Per favor, escollisca una clau per utilitzar:
ID de Clau
ID de usuari
0F858DE1 Xavier Orduña Just ((Compte UPC)) <xavier.orduna@upc.es>
4FD5684F Xavier Orduña Just ((Enllac)) <xavi@enllac.com>
7EDE8BAD XorA Just <xora_just@hotmail.com>
BBBD9492 Xavier Orduña <xora@telefonica.net>
CA212C08 paranoic1 <paranoic1@jabber.upc.es>
Cancel·lar
Bé
Clau pública: paranoic1@jabber.upc.es
Per favor, escollisca una clau per utilitzar:
ID de Clau
ID de usuari
47A14ED0 Enric Font Segarra (Killu) <killu@eresmas.com>
4A89C248 poveda (fastcallforall) <landeresp@netscape.net>
4FD5684F Xavier Orduña Just ((Enllac)) <xavi@enllac.com>
69AB5784 Manuel Lucena Lopez <mlucena@ujaen.es>
7EDE8BAD XorA Just <xora_just@hotmail.com>
CA212C08 paranoic1 <paranoic1@jabber.upc.es>
Cancel·lar
Bé

Tkabber

- **Basat en Tcl/Tk**
  - **Multiplataforma.**
- **OpenPGP integrat**
- **Aprofita quasi totes les capacitats del protocol jabber**
- **http://tkabber.jabber.ru**

Exemple de Conversa

Exemple de conversa(2)



Problemes

- **Lliguem el xifrat de converses al PC on tinguem les claus privades.**
  - **Servidor de claus privades?**
- **Genera un tràfic descomunal**
  - **Un espai pot ocupar 500 caràcters**
- **Implica fer treballar constantment la CPU**
  - **Si ens en sobra, cap problema**

Conclusions

- **Tenir converses xifrades està a l'abast de tothom**
- **A vegades pot resultar innecessari**
- **No es pot deixar que certs organismes es creguin amb el dret de interceptar missatges**

Bibliografia

- www.jabber.org
- www.jabberes.org
- www.openpgp.org
- www.gnupg.org
- winpt.sf.net
- www.google.com

Enric Font Segarra
(boladepalla@jabber.org)

Xavier Orduña Just
(xavi@jabber.upc.es)

Maig 2004