

GnuPG: criptografía para todos

Diego Berrueta Muñoz
berrueta@asturlinux.org

Marzo 2001



Contenido

- / Introducción a la criptografía de clave pública
- / Presentación de GnuPG
- / Utilización de GnuPG
- / Intercambio de claves y anillos de confianza
- / GnuPG y programas auxiliares
- / Usos habituales de GnuPG



Tipos de cifrado

- / Simétrico (clave privada)
- / Asimétrico (clave pública)

Se diferencian principalmente en:

- / El número de claves
- / La distribución de las claves
- / El uso de las claves en el algoritmo

Ninguno es inherentemente superior al otro



Cifrado simétrico

- / Emisor y receptor comparten una única clave (secreta), que sirve tanto para cifrar como para descifrar el mensaje.
- / Su debilidad está en el intercambio de claves, no en el algoritmo en sí. Si n personas quieren intercambiar mensajes, se necesitan $n(n-1)/2$ claves.
- / Son algoritmos de cifrado simétrico: IDEA, 3DES, Blowfish... y “Enigma”.



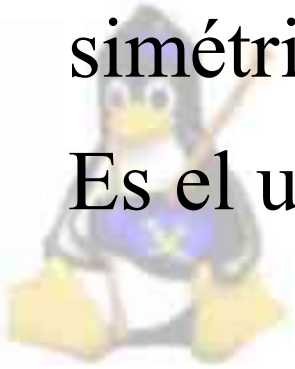
Cifrado asimétrico (clave pública)

- / Cada usuario tiene dos claves: una pública y una privada.
- / Lo que se cifra con una de las claves, sólo se puede descifrar con la otra.
- / La clave pública se distribuye libremente.
- / Toda la seguridad del sistema depende de la seguridad de la clave, no del algoritmo.

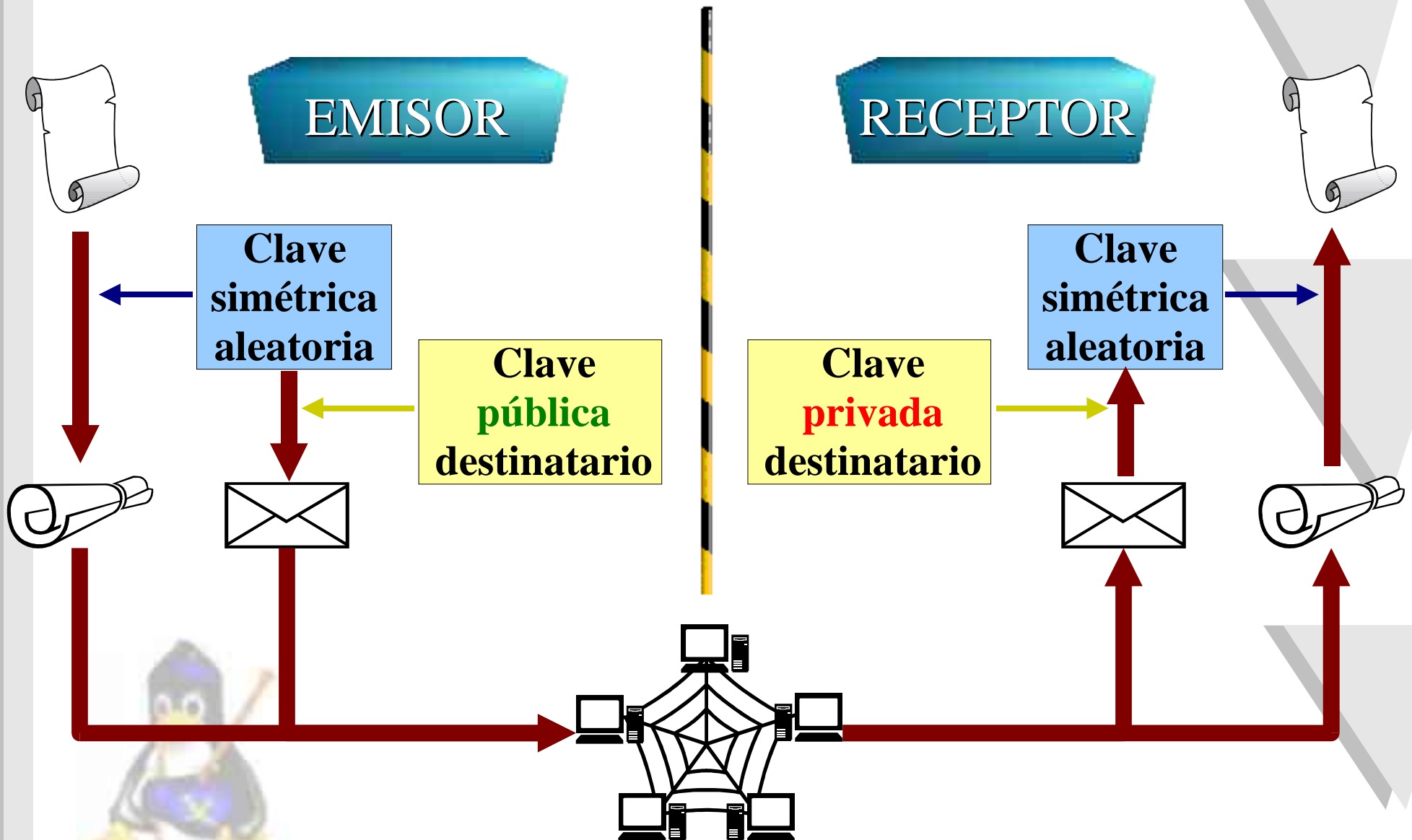


Cifrado híbrido

- / Utiliza un cifrado simétrico y otro asimétrico.
- / Se cifra el mensaje con un algoritmo simétrico, y se envía la clave cifrada a su vez con un algoritmo asimétrico.
- / La clave del algoritmo simétrico es de “*usar y tirar*”.
- / Externamente, se comporta como un cifrado simétrico.
- / Es el usado por GnuPG y PGP.



Envío de un mensaje cifrado

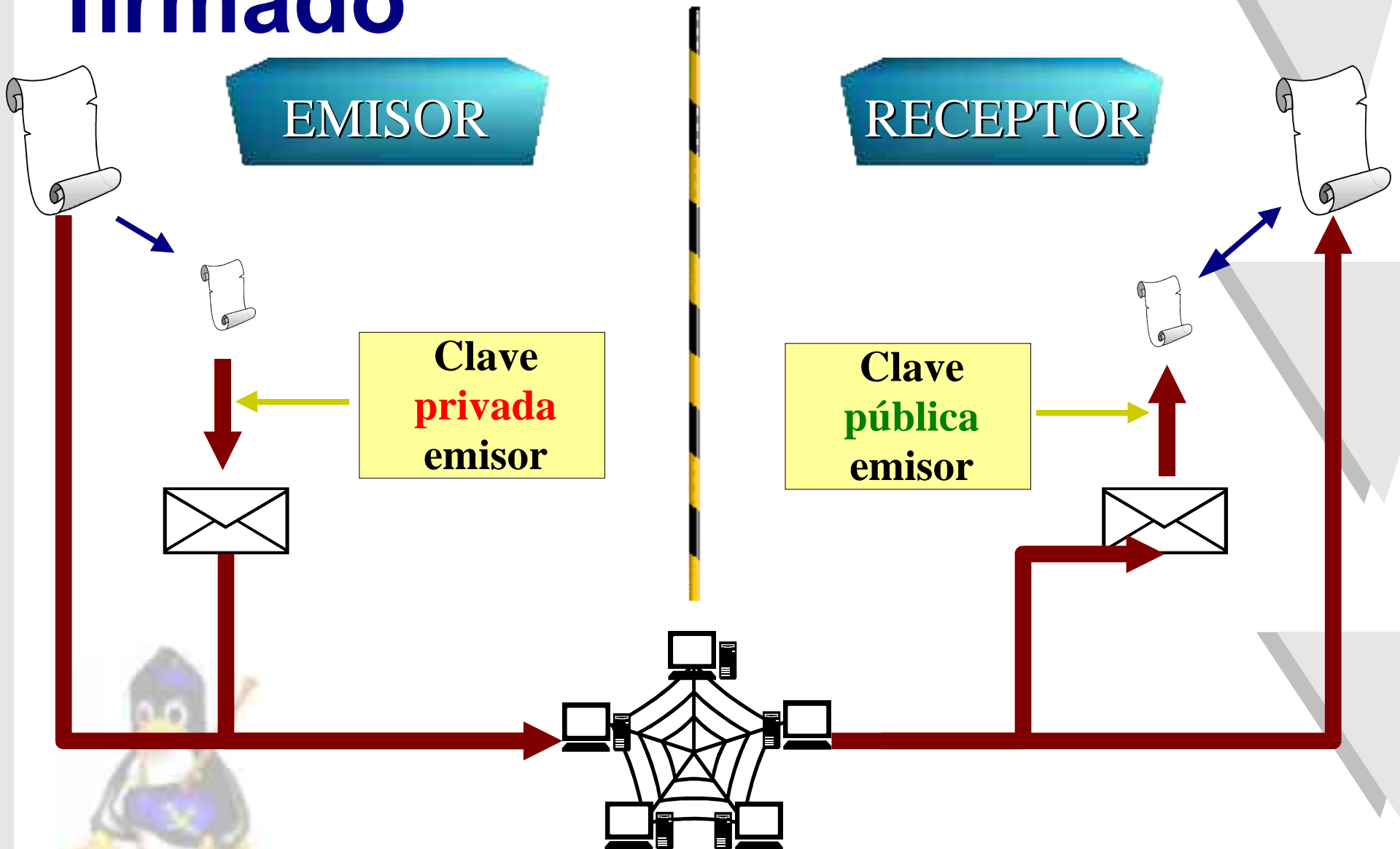


Firma digital

- / Se utiliza una función *hash* para obtener un “resumen” del mensaje.
- / El emisor cifra con el resumen con su clave privada.
- / Cualquiera que posea la clave pública del emisor puede descifrar el resumen y comprobar si coincide con el resumen del mensaje que ha recibido.



Envío de un mensaje firmado



¿Qué es GnuPG?

- " GnuPG es una herramienta criptográfica esencialmente compatible con PGP, y distribuída bajo licencia GPL.
- " GnuPG no utiliza algoritmos patentados (IDEA, RSA).
- " GnuPG es desarrollado abiertamente, y el gobierno alemán colabora económicamente en el proyecto.



Ventajas de GnuPG

- / Es software libre, se puede modificar, corregir, ampliar...
- / Es software desarrollado en Europa, evitando así las incómodas restricciones de los EEUU a la exportación de software criptográfico.
- / Es compatible con el estándar OpenPGP.
- / Está disponible en multitud de sistemas.
- / Se puede usar con fines personales y comerciales.



Anillos de claves

- / GnuPG almacena nuestra clave privada y pública (pueden ser varias).
- / También almacena las claves públicas de otras personas.
- / Estos almacenes se llaman *anillos de claves*.
- / En UNIX, se almacenan en `~/ .gnupg`
- / La clave privada está protegida con un cifrado simétrico.
- / GnuPG puede importar anillos de claves de PGP.



Operaciones básicas

/ Cifrar

```
gpg --encrypt [fichero] --recipient [uid]
```

/ Descifrar

```
gpg --decrypt [fichero]
```

/ Firmar

```
gpg --sign [fichero]
```

/ Verificar firma

```
gpg --verify [fichero]
```



Opciones habituales

/ Desviar la salida a un fichero:

`-o [fichero]`

/ Forzar salidas ASCII de 7 bits:

`--armor`

/ Firmar en un fichero aparte:

`--detach-sign [fichero]`

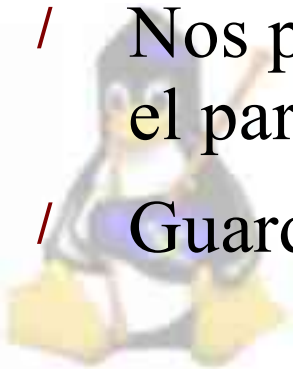


Generación de una clave

- / Generar un nuevo par de claves pública/privada:

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

- / Nos pide el algoritmo a usar (recomienda DSA/ElGamal).
- / Nos pide la longitud de la clave (768-2048 bits).
- / Nos pide el nombre y dirección de correo.
- / Nos pide una *passphrase* (contraseña larga).
- / Nos pide que aumentemos la entropía mientras genera el par de claves.
- / Guarda las nuevas claves en el anillo de claves.



Exportación e importación de claves (públicas)

/ Exportación de una clave (o varias):

```
gpg --export [UID] [--armor]
```

/ Si se omite el UID, exporta todas las claves públicas de nuestro anillo.

/ Importación de una clave (o varias):

```
gpg --import [fichero]
```



Administración de claves

- / Ver las claves de nuestro anillo:

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

- / Borrar una clave pública de nuestro anillo:

```
gpg --delete-key UID
```

- / Borrar una clave privada de nuestro anillo:

```
gpg --delete-secret-key
```

- / Editar una clave:

```
gpg --edit-key UID
```



Edición de claves

Nos permite:

- / Firmar una clave.
- / Modificar la fecha de caducidad.
- / Añadir una huella digital (*fingerprint*).
- / Añadir y borrar identificativos de usuario.
- / Modificar el grado de confianza en la clave.
- / Cambiar la *passphrase*.



Intercambio de claves

- / El problema de los sistemas de clave pública no es el intercambio de claves, sino cómo estar seguros de que las claves pertenecen a quien nosotros creemos que pertenecen.
- / El único medio realmente seguro es intercambiar las claves personalmente.
- / NO son seguras las claves recibidas por correo electrónico, descargadas por FTP o desde una página web.



Confianza en las claves

- / Cada clave pública de nuestro anillo tiene asociado un grado de confianza (*trust*).
- / Las claves en las que confiamos plenamente, podemos marcarlas como “confianza plena”.
- / También existen los grados de confianza “marginal”, “nula” y “no lo sé”.
- / Inicialmente, la confianza es “no lo sé”.



Huellas digitales (fingerprints)

- / Son un medio de aumentar la confianza en una clave.
- / Consisten en un resumen de 160 bits de la clave.
- / Cada clave tiene una huella digital única.
- / Nos pueden servir para comprobar claves en persona, por teléfono, etc.



Firma de claves

- / Es un método para comunicar a una persona la clave de un tercero.
- / Podemos firmar aquellas claves ajenas en las que confiemos.
- / Luego enviamos la clave firmada a otra persona, que la añadirá a su anillo si confía en nuestra firma y confía en nosotros.
- / Cuantas más personas firmen nuestra clave, más confiará la gente en ella.



Anillos de confianza

- / Son un método para hacer que nuestra clave pública sea firmada por muchas personas.
- / Consisten en crear un repositorio de claves públicas de multitud de personas.
- / Todos los participantes aportan su clave pública y firman las claves públicas de todos los demás.
- / Una vez establecido el anillo, es fácil seguir incorporando claves.
- / Es esencial seguir un procedimiento seguro.



Algunos usos habituales de GnuPG

- / Enviar y recibir correo electrónico firmado y cifrado.
- / Comprobar la autenticidad del software que descargamos de la red (núcleo, parches, paquetes deb/rpm...).
- / Guardar nuestras contraseñas de forma segura.
- / Sistemas de votación electrónica (Debian).



GnuPG y otros programas

/ Clientes de correo con soporte GnuPG:

- / Mutt
- / Kmail
- / Evolution (≥ 0.9)
- / Pine (pgp4pine)
- / ...

/ Otras herramientas (front-ends):

- / GPA
- / gpgp
- / TkPGP



- / ...

Mutt (I)

- / Cliente de correo para consola.
- / Se integra perfectamente con GnuPG y PGP.
- / Reconoce los mensajes que llegan firmados (o cifrados) y verifica la firma (o descifra) automáticamente.
- / Indica con precisión dónde comienzan los datos firmados (o cifrados) y dónde terminan.



Mutt (enviar mensaje)

```
Terminal
Archivo  Editar  Configuración  Ayuda
y:Mandar  q:Abortar  t:To  c:CC  s:Subj  a:Adjuntar archivo  d:Descrip  ?:Ayuda
  From: Diego Berrueta <berrueta@asturlinux.org>
  To: asturlinux@asturlinux.org
  Co:
  Bcc:
  Subject: presento mi dimisión
  Reply-To:
  Fcc:
  Mix: <no chain defined>
  PGP: En claro

-- Archivos adjuntos
- I /tmp/mutt-poketa-915-1 [text/plain, 7bit, us-ascii, 0.3k]

-- Mutt: Crear mensaje
co(d)ificar, f(i)rmar (c)omo, amb(o)s, escoger algoritmo (m)ic, ca(n)celar
```

Mutt (recibir mensaje)



```
mutt
Archivo  Editar  Configuración  Ayuda
i:Salir  -:PágAnt <Space>:Pró:Pág  v:Adjuntos  d:Sup.  r:Responder  j:Sig.  ?:A
From: laespiral-request@matrio.com  Sun Mar 11 14:53:11 2001
Date: Sun, 11 Mar 2001 14:55:47 +0100
From: Javier Viñuales Gutiérrez <vigu@matrio.com>
Subject: Re:
Reestructuración del CD 2, está un poco mejor :)
To: laespiral@matrio.com

[-- Salida de PGP a continuación (tiempo actual: Fri Mar 16 18:40:39 2001) --]
gpg: Firma creada el dom 11 mar 2001 14:55:47 CET usando clave DSA ID 4EB82468
gpg: Imposible comprobar la firma: Clave pública no encontrada
[-- Fin de salida PGP --]

[-- Los siguientes datos están firmados --]

On sáb, mar 10, 2001 at 09:31:54 +0100, Manel Marin wrote:
> ¿Hay un listado más reciente (URL)? Lo siento no he podido ponerme antes...
Pues no, no me ha dado tiempo pero esta noche lo pongo.

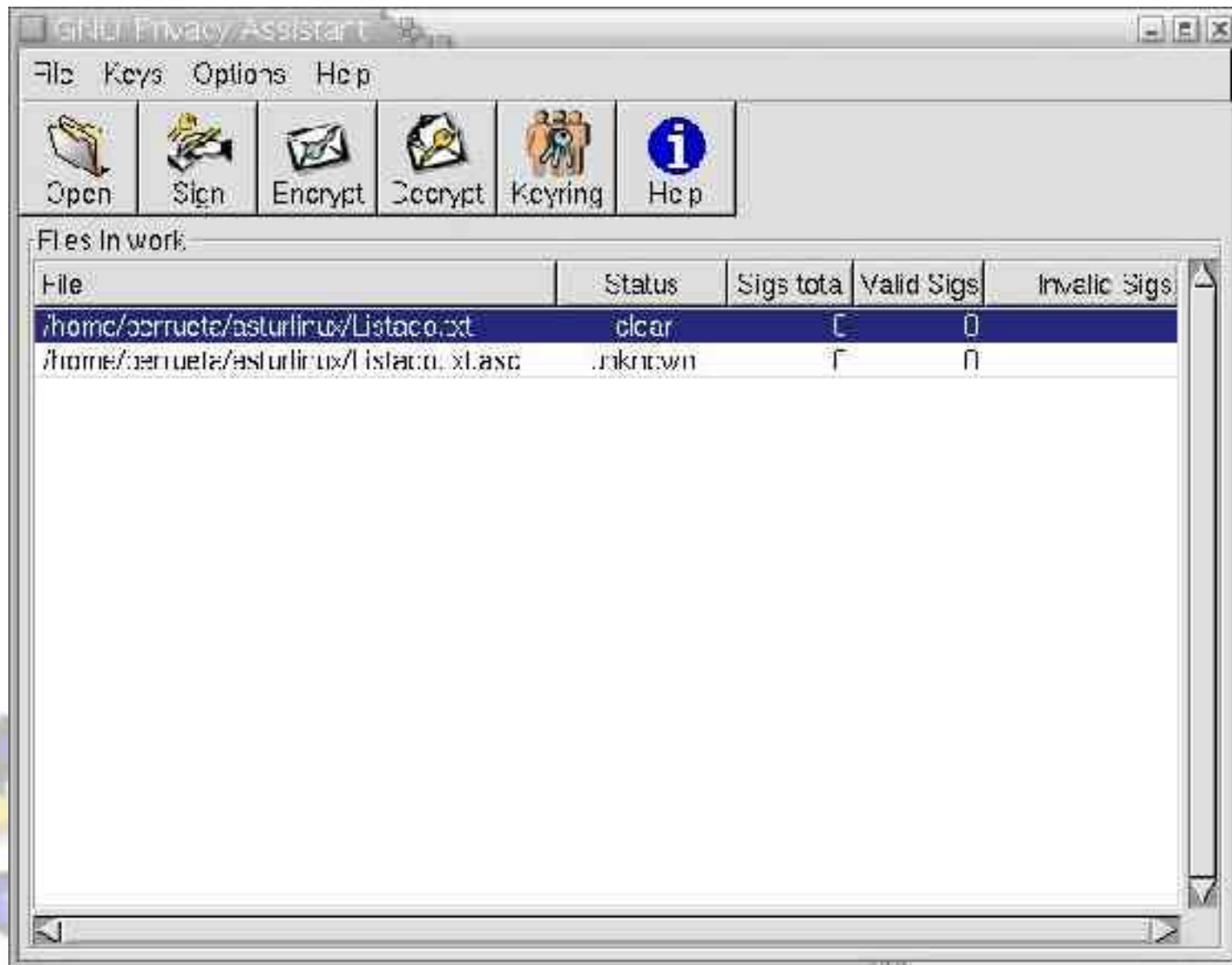
> Así de entrada veo que falta la actualización de seguridad de openssh, yo
> podría repasar que estén todas las actualizaciones de seguridad ¿sí?
- s - 5/13: Javier Viñuales Guti  Re: Reestructuración del CD 2, está -- (46%)
```

GPA

- / Es un front-end gráfico que facilita el uso de GnuPG.
- / Soporta la gran mayoría de opciones y posibilidades de GnuPG (especialmente las más utilizadas).
- / Es cómodo de usar.
- / Está programado con GTK, por lo que es muy portable.



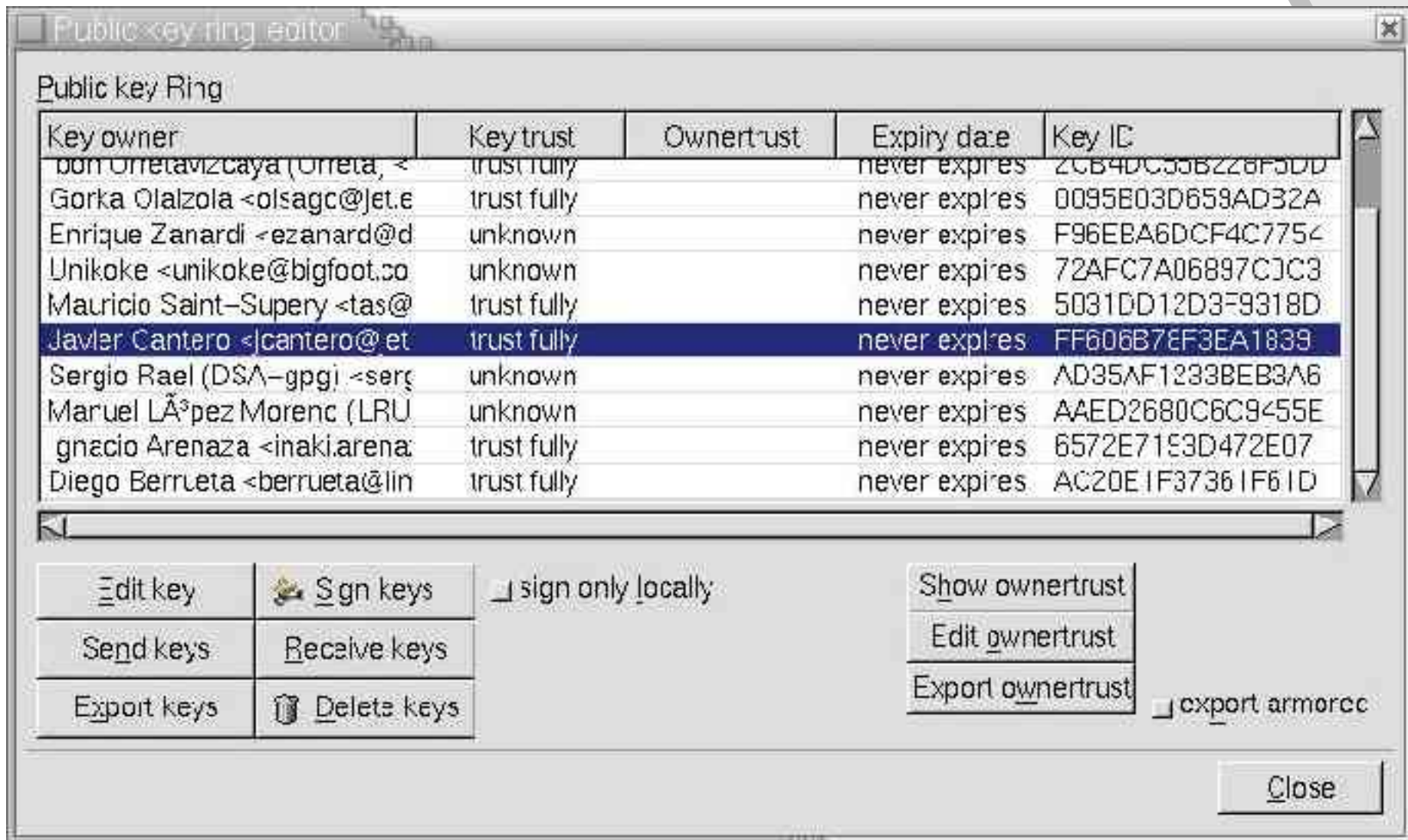
GPA (pantalla principal)



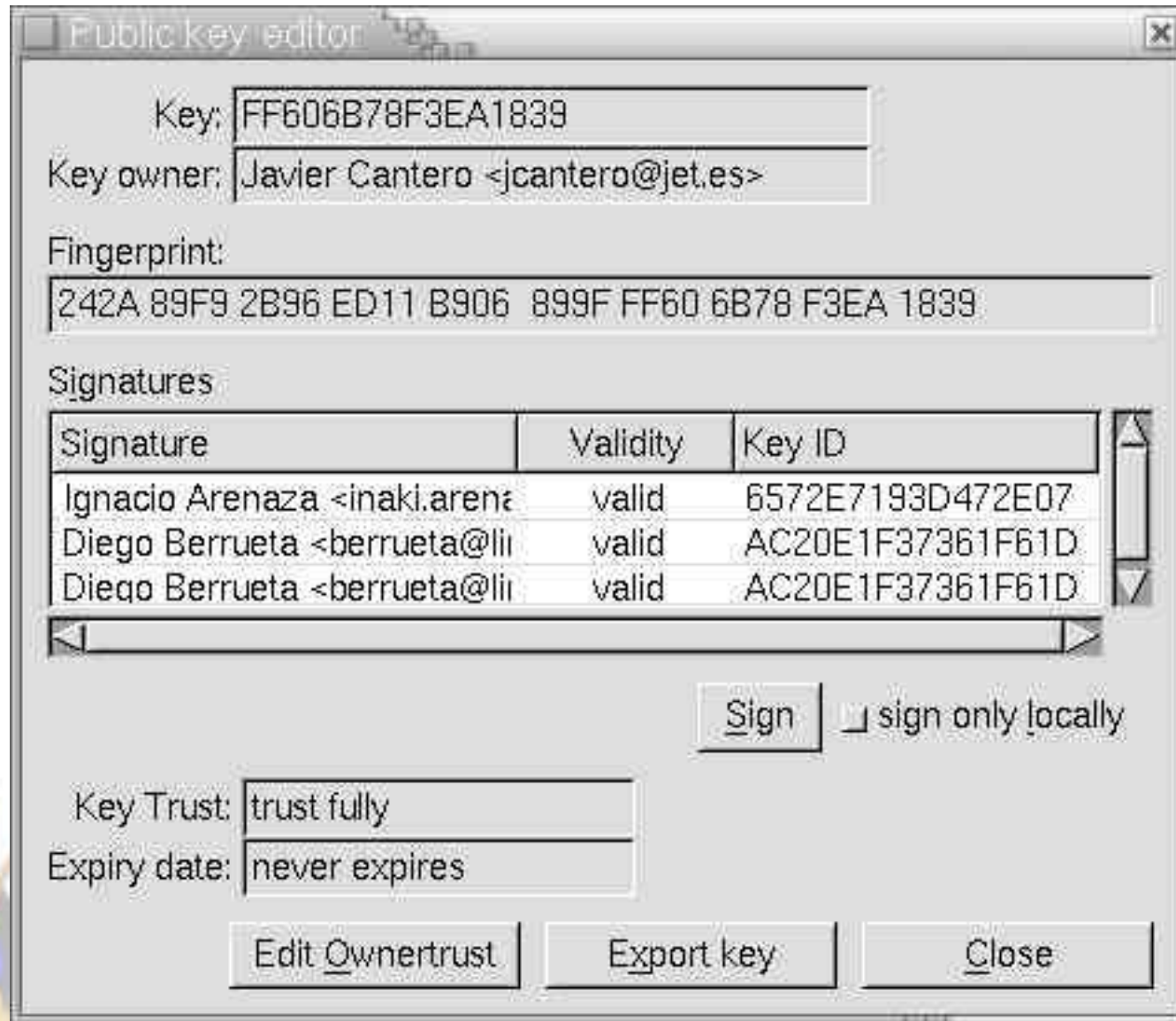
GPA (opciones del menú)



GPA (anillo de claves)



GPA (edición de clave)



Referencias

- / GnuPG: <http://www.gnupg.org/>
- / Manual de GnuPG (disponible en español)
- / GnuPG HOWTO: <http://www.linuxdoc.org/>
Versión traducida al español: <http://www.insflug.org/>
- / GPA: <http://www.gnupg.org/>
- / Mutt: <http://www.mutt.org/>

