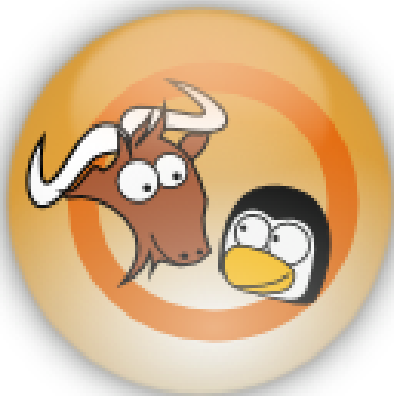


GnuPG - GNU Privacy Guard



GnuPG - GNU Privacy Guard

Julio Herrero

`julher@escomposlinux.org`

Galpon - Grupo de Amigos de Linux de Pontevedra

Vigo, 11 de abril de 2015

Contenido

- 1 Conceptos
 - GnuPG
 - Características
- 2 Uso de GnuPG
 - Instalación
 - Creación de claves
 - Opciones
 - Cientes de correo
 - Fiesta de firmado de claves

Contenido

- 1 Conceptos
GnuPG
Características

GnuPG



¿Que es GnuPG? (Según la wikipedia)

GNU Privacy Guard (GnuPG o GPG) es una herramienta de cifrado y firmas digitales, que viene a ser un reemplazo del PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenPGP.

Claves

- Sirve para cifrar y firmar digitalmente sustituyendo a PGP
- Es software libre (GPL)
- Implementa el estándar OpenPGP del IETF





[Home](#) [Donate](#) [Download](#) [Documentation](#) [Related software](#) [Blog](#)

[Features](#) [News](#) [People](#) [Service](#)

THE GNU PRIVACY GUARD

GnuPG is a complete and free implementation of the OpenPGP standard as defined by [RFC4880](#) (also known as *PGP*). GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as *GPG*, is a command line tool with features for easy integration with other applications. A wealth of [frontend applications](#) and



Según ellos mismos. . .

GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also known as PGP). GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features. . .



¿Y que es PGP?

Pretty Good Privacy o PGP (privacidad bastante buena) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

- <http://www.pgp.com>



Versiones

- 1.X versión original
- 2.X versión moderna
- última estable es la 2.0.26
- última disponible 2.1.26



Características

- Básicamente es una herramienta en modo de línea de comando
- hay front-ends para quien quiera:
- `https://www.gnupg.org/related_software/frontends.html`



Sistemas operativos soportados

Está soportado en los tres grandes SO actuales: Linux, MacOS X y Windows. Compila en *BSD y en las siguientes plataformas

- AIX
- HPUX
- IRIX
- SCO
- SunOS
- ...



¿Donde está el código?

- <https://www.gnupg.org/download/mirrors.html>

¿Donde está la documentación?

Howto, manuales, guías de usuario, listas de correo, FAQ...

- <https://www.gnupg.org/documentation/index.html>



Sistemas criptográficos

Las dos grandes familias

- **Cifrados simétricos:** se usa una clave secreta
- **Cifrados asimétricos:** se usan dos claves, una pública y una privada

El sistema híbrido

- Un sistema de cifrado híbrido usa tanto cifrado simétrico como asimétrico simultáneamente.
- Funciona mediante el uso de un cifrado de clave pública para compartir una clave para el cifrado simétrico
- La clave simétrica usada es diferente para cada sesión.



Sistemas criptográficos

GnuPG

- Tanto PGP como GnuPG usan sistemas de cifrado híbridos
- La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, de manera automática.
- El destinatario usa su clave privada para descifrar la clave de sesión y acto seguido usa la clave de sesión para descifrar el mensaje.



Sistemas criptográficos

¿Y como sabemos que una clave es de quien dice ser?

- Confiar en autoridades de certificación (certificados X509)
- En gnupg no hay autoridades, son los usuarios que en base a sus **firmas de claves** establecen el grado de confianza en una clave determinada.



¿vale la pena?

<https://emailselfdefense.fsf.org/es/>



Contenido

2 Uso de GnuPG

- Instalación

- Creación de claves

- Opciones

- Cientes de correo

- Fiesta de firmado de claves



Instalación

Instalación

- **Linux:** Mediante los gestores de paquetes de las distribuciones (apt. . .) o compilando las fuentes
- **Sistemas propietarios:** normalmente hay software compilado listo para instalarse (GPGTOOLS en Mac, GPG4WIN en Windows...)
- También hay software para **Android e IOS.**



Instalación con apt

```
#apt-get install gnupg2
```

```
Leyendo lista de paquetes...
```

```
Creando árbol de dependencias...
```

```
Leyendo la información de estado...
```

```
Se instalarán los siguientes paquetes extras:
```

```
gnupg-agent libassuan0 libatk1.0-0 libatk1.0-data
```

```
libcurl3-gnutls libgtk2.0-0 libgtk2.0-bin ...
```



GPG4WIN (<http://gpg4win.org>)



GPGTOOLS (<https://gpgtools.org>)



The screenshot shows the homepage of the GPG Tools website. At the top left is the GPG Tools logo, which consists of a blue padlock icon and the text "GPG TOOLS". To the right of the logo is a navigation menu with links for "GPG Suite", "Donate", "News", "Download Suite", and "Support", followed by a Twitter icon. The main content area has a dark blue background with a white icon of an open box. The text "GPG Suite" is prominently displayed. Below this, there is a paragraph: "Everything you need to get started with secure communication and encryption lies in one simple package." To the right of this paragraph, it says "For OS X 10.10 Yosemite" and "Compatible back to OS X 10.8". A red button with a white download icon and the text "Download GPG Suite" is positioned to the right of the main text. At the bottom of the page, there is a small paragraph: "Use GPG Suite to encrypt, decrypt, sign and verify files or messages. Manage your GPG keychain with a few simple clicks and experience the full power of GPG easier than ever before."



Instalación

Android (<https://guardianproject.info/code/gnupg/>)



Creación de claves

```
$ gpg2 --gen-key
gpg (GnuPG) 2.0.26; Copyright (C) 2013 Free Software
Foundation, Inc. This is free software: you are
free to change and redistribute it. There is NO
WARRANTY, to the extent permitted by law.
Seleccione tipo de clave deseado:
(1) RSA y RSA (predeterminada)
(2) DSA y ElGamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
Su elección: 1
```



Creación de claves

las claves RSA pueden tener entre 1024 y 4096 bits de longitud.

¿De qué tamaño quiere la clave? (2048)

Especifique el período de validez de la clave.

0 = la clave nunca caduca

<n> = la clave caduca en n días

<n>w = la clave caduca en n semanas

<n>m = la clave caduca en n meses

<n>y = la clave caduca en n años



Creación de claves

GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Julio Herrero

Dirección de correo electrónico:

altamar@jherrero.org

Comentario: Clave de pruebas para charla de Galpon

Necesita una contraseña para proteger su clave secreta.



Creación de claves

Es necesario generar muchos bytes aleatorios. Es una buena idea realizar alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar la red y los discos) durante la generación de números primos. Esto da al generador de números aleatorios mayor oportunidad de recoger suficiente entropía.



Creación de claves

```
gpg: clave DF966566 marcada como de confianza
absoluta
Huella de clave = 87B2 77C0 EC08 7B99 752E F367 6FDA
5BAC DF96 6566
uid [ absoluta ] Julio Herrero (Clave de pruebas para
charla de Galpon) <altamar@jherrero.org>
```



Opciones básicas

- `man gpg2`
- La configuración y claves en `$HOME/.gnupg`
- Ya podemos cifrar (`--encrypt`), descifrar (`--decrypt`), firmar (`--sign`, `--sign-key`) ...
- Hay disponibles servidores públicos de claves (`--recv-keys`, `--search-keys`, `--send-keys`, `--keyserver`)



Cientes de correo

Ejemplos

- **Mutt**: se configura el ID de la clave en `.muttrc` (y más)
- **Evolution**: cliente de correo de Gnome con GnuPG soportado de manera nativa.
- **Thunderbird**: Ciente disponible en varios SO. Hay que instalar el complemento Enigmail.
- **Mail**: Cliente nativo de MacOS X. Hay que instalar GPGTOOLS.



Evolution

debian-user (18 no leídos, 19 en total) - Evolution

Archivo Editar Ver Mensaje Carpeta Buscar Ayuda

Nuevo Enviar / Recibir Responder Responder al grupo Reenviar

debi... 18 no leídos, 19 en total Buscar: El asunto o las direcciones contienen en Carpeta actual

De	Asunto	Fecha
claude juif <claude.juif@g...>	Re: free cloud	Hoy 16:12
Nate Bargmann <n0nb...>	Re: free cloud	Hoy 15:51
claude juif <claude.juif...>	Re: free cloud	Hoy 16:17

Re: free cloud (De: claude juif <claude.juif@gmail.com>)

2015-04-08 16:09 GMT+02:00 Lisi Reisz <lisi.reisz@gmail.com>:
On Wednesday 08 April 2015 14:07:45 Chris Bannister wrote:
> > On Tue, Apr 07, 2015 at 05:02:17PM -0700, Joris Bolsens wrote:
> > > On 04/02/2015 03:58 PM, Bernd Naumann wrote:
> > > > But the downside on all these 'cheep vps provider' I'm aware off,
> > > > is that they don't offer any useful amount of storage space. So
> > > > maybe find a friend or too, and invest in a monthly rent of a
> > > > bare-metal-server ;)
> > > >
> > > > honestly some of the cheaper dedi's aren't even that expensive



Evolution

Editor de cuentas

Identidad
Recepción de correo
Opciones de recepción
Envío de correo
Predeterminados
Seguridad

General

- No firmar las solicitudes de reunión (para compatibilidad con Outlook)

Pretty Good Privacy (OpenPGP)

ID de clave OpenPGP:

Algoritmo de firma: Predeterminado ▾

- Firmar siempre los mensajes salientes cuando se use esta cuenta
- Siempre cifrar a mí mismo cuando envíe correo cifrado
- Siempre confiar en las claves de mi almacén al cifrar

MIME seguro (S/MIME)

Certificado de firma:

Algoritmo de firma: Predeterminado ▾

- Firmar siempre los mensajes salientes cuando se use esta cuenta

Certificado de cifrado:

- Cifrar siempre los mensajes salientes cuando se use esta cuenta
- Ciframe siempre a mí mismo cuando envíe correo cifrado





julio@x101: ~ debian-user (18 no leí... Preferencias de Evoluti...



Evolution

prueba de gpg

Archivo Editar Ver Insertar Formato Opciones

Enviar    

De: julHer <julher@escompostlinux>


Para: altamar@jherrero.org

Cc:

Asunto: prueba de gpg

Firmar con PGP
 Cifrar con PGP
 Firmar con S/MIME
 Cifrar con S/MIME
 Solicitar confirmación de lectura
 Priorizar mensaje

Codificación de caracteres ▶

Texto plano ▼ Normal ▼ 

asdfadsf afasfd
asfa fd df adffas
ad fafas s
|

▶ Mostrar barra de adjuntos Añadir adjunto... Vista de icono ▼



Thunderbird

The screenshot shows the Thunderbird email client interface. The window title is "asterisk". The top toolbar includes "Recibir mensajes", "Redactar", "Charlar", "Direcciones", "Etiqueta", "Filtro rápido", and a search bar. The left sidebar shows a folder tree with folders like "Bandeja de entrada", "Borradores", "Enviados", "Papelera", "asterisk (4)", "coit", "debian (6)", "debian-french (6)", "debian-ppc (16)", "debian-user (24)", "Deleted Messages", "ecol", "esa (2)", "exim", "galpon", "julio", "kripto", "mapas", "Notes", "owncloud (8)", "Queuo", "sailfish (4)", "seguridad (4)", "sistema (5)", "sorpresa", "spem", "vaughan", "Carpeta local", "Papelera", and "Bandeja de salida".

The main pane displays an email with the following details:

- Asunto:** Re: [asterisk-users] WEBRTC is no longer working with Firefox after upgrade to version 37
- De:** Joshua Colp <jcolp@digium.com>
- Asunto:** Re: [asterisk-users] WEBRTC is no longer working with Firefox after upgrade to version 37
- A:** Asterisk Users Mailing List - Non-Commercial Discussion <asterisk-users@lists.digium.com>

The email body contains the following text:

Toufic Khreish (Gmail) wrote:
Hello,

Webrtc stopped after upgrading firefox from version 36 to version37. I have been running webrtc with freepbx 12 and asterisk 13.2 or 13.3 and firefox version 36 without any issues until firefox was upgraded to version 37. Unfortunately Chrome works well in one direction (from chrome to any extension) but calling from an extension to a webrtc on chrome has one way voice.

Could someone try to investigate the problem of firefox version37.0.1 with webrtc ? no voice in any direction. Should we try it with a computer that has not an updated version of firefox things work normally, also if we rollback (install version 36, it works well)

Someone already filed an Asterisk issue[1] and there is also a Firefox issue[2]. It's also been fixed in Firefox 38 already.

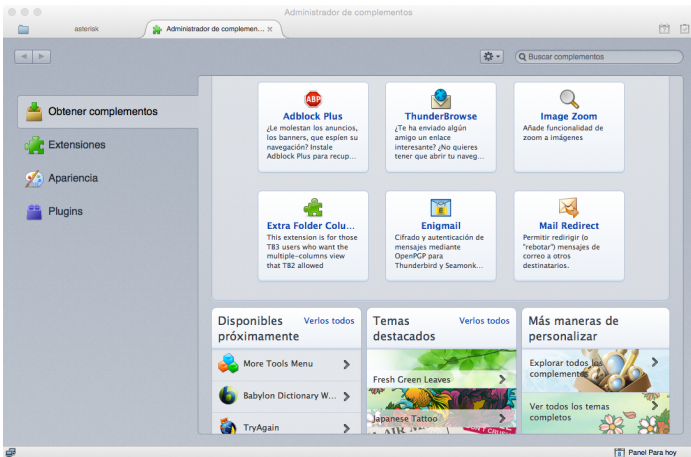
[1] <https://issues.asterisk.org/jira/browse/ASTERISK-24911>
[2] https://bugzilla.mozilla.org/show_bug.cgi?id=1147919

Joshua Colp
Digium, Inc. | Senior Software Developer

The bottom status bar shows "Sin leer: 4", "Total: 5", and "Panel Para hoy".



Thunderbird



Thunderbird

The screenshot shows the Thunderbird Add-on Manager window. The title bar reads "Administrador de complementos". The main content area displays the details for the "Enigmail 1.8.1" extension by Patrick Brunschwig. The extension is described as providing encryption and authentication for messages using OpenPGP. It includes a green "Add to Thunderbird" button and a "Más información" button. Below the description is a small screenshot of the extension's interface. The extension has a rating of 4.5 stars from 179 users, with 134,620 active users and a last update date of March 26, 2015. The website link is <http://enigmail.mozdev.org/>. A "Valoraciones" section contains user feedback.

Administrador de complementos

Obtener complementos

Extensiones

Apariencia

Plugins

Enigmail 1.8.1
por [Patrick Brunschwig](#) [▲ Volver a complementos](#)

Cifrado y autenticación de mensajes mediante OpenPGP para Thunderbird y Seamonkey. Requiere GnuPG (www.gnupg.org).

[+ Add to Thunderbird](#) [Más información](#)

Calificación ★★★★☆ 179 valoraciones

Usuarios activos 134.620

Últimos actualizados March 26, 2015

Página web <http://enigmail.mozdev.org/>

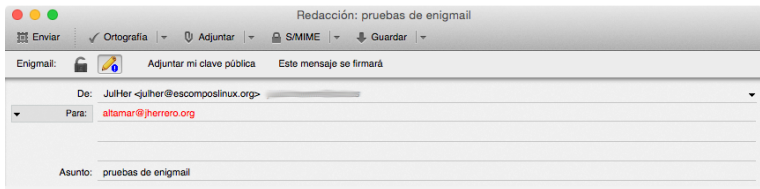
Valoraciones

Good but since version 1.8 the ugliest addon... Great extension, been using it for year, but, seriously, who had the idea for that toolbar in the compose window? That's the ugliest thing I have ever seen. As an option for those with really poor eyesight okay but not as the only

Panel Para hoy



Thunderbird



adsadf asdfasdf
afdadf adsfasf
a fdasfa asdf



Mail

The screenshot shows a mail client window titled "debian-user" with 30 messages and 28 unread. The left sidebar lists folders like "Entrada", "Contactos VIP", "Enviado", "No deseado", "Papeleria", and "Deleted Messages". The main pane shows a list of emails, with the selected one from Vincent Lefevre. The detailed view of the email shows the following content:

Vincent Lefevre
Para: debian-user@lists.debian.org
Reenviado por: debian-user@lists.debian.org
ssh hangs for 5 seconds for a particular machine

8 de abril de 2015, 19:11

When connecting by SSH to a particular machine, ssh hangs for 5 seconds. The client machine doesn't matter (except for the machine itself). For instance:

```
xvii:~> ssh -vvv 2>>(ts -s "%s") ypig
[...]
```

0.278462 debug2: key: /home/vinc17/.ssh/id_rsa (0x7f943e415e90), explicit
0.278513 debug2: key: rsa w/o comment (0x7f943e418a60),
0.278553 debug2: key: rsa w/o comment (0x7f943e418620),
0.278591 debug2: key: /home/vinc17/.ssh/id_rsa-internal ((nil)), explicit
5.291295 debug1: Authentications that can continue: publickey,password
[...]

This is always reproducible and this problem had never occurred before today.

Any idea?

Vincent Lefèvre <vincent@vinc17.net> - Web: <<https://www.vinc17.net/>>
100% accessible validated (X)HTML - Blog: <<https://www.vinc17.net/blog/>>
Work: CR INRIA - computer arithmetic / Aric project (LIP, ENS-Lyon)

To UNSUBSCRIBE, email to debian-user-REQUEST@lists.debian.org
with a subject of "unsubscribe". Trouble? Contact
listmaster@lists.debian.org
Archive: <https://lists.debian.org/20150408171107.GA22873@xvii.vinc17.org>

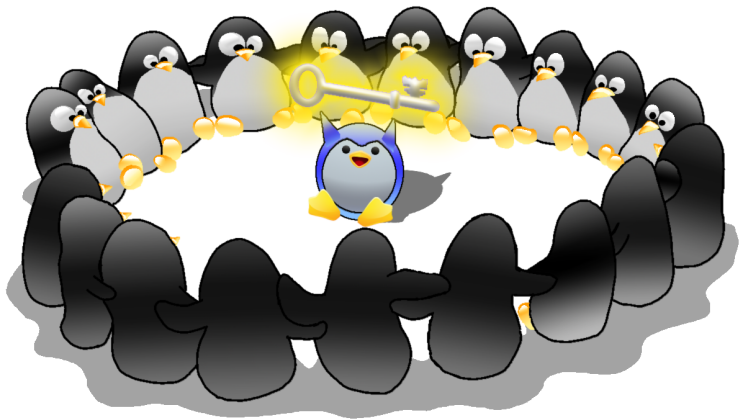


Mail



asda asdfadsf asdfasfd asdf asdf
asdasdf asdfasdfa asdfasdf

Key signing party



Key signing party

¿En que consiste?

Una fiesta de firmado de claves es una reunión de personas usuarias o interesadas en la criptografía proporcionada por GnuPG para firmarse mutuamente las claves, previa verificación de la identidad, y de esa manera establecer anillos de confianza.

¿Que hay que llevar?

- El ID de la clave.
- La huella de la clave.
- Dos identificaciones personales.
- No están bien vistos los ordenadores en esas fiestas.



Key signing party



Key signing party

Chuletario

- Enviar clave a servidor: `gpg2 --send-keys ID`
- Obtener clave de servidor: `gpg2 --recv-keys ID`
- Firmar clave: `gpg2 --sign-key ID`
- Exportar firma clave para enviar: `gpg2 --armor --output archivo.asc --export ID`
- Importar firma clave recibida: `gpg2 --import archivorecibido.asc`
- Ver las firmas de una clave: `gpg2 --list-sigs ID`



¿aburridos?



#SLAltamar

