Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Mutt y GPG en cinco minutos (10445 lectures)

Per **Celso González**, ***PerroVerd*** (http://mitago.net)

Creado el 13/12/2001 20:24 modificado el 13/12/2001 20:24

En este artículo explico como partiendo de un cliente de correo mutt funcionando podemos añadirle la potencia de GPG para **firmar** o **cifrar** nuestros mensajes de correo electrónico

10 pasos para instalar GPG+Mutt

- Instalar el paquete gpg. Si estamos en debian hacemos `apt-get install gpg` y si estamos en una distro rpm bajamos el paquete de rpmfind.net[1] y hacemos `rpm -i gnupg-xxxx.rpm`
- Generar nuestras claves, para hacer esto tecleamos `gpg --gen-key`
- Ahora nos pide el tipo de clave que queremos generar, usualmente da a elegir entre DSA (para firmar), ElGamal (para cifrar) o las dos a la vez. En nuestro caso seleccionamos que nos genere los 2 tipos de clave.
- Seguidamente, debemos introducir el tamaño de la clave ElGamal que queremos generar, como hay mucho paranoico elegimos el máximo posible 2048
- El siguiente paso es elegir la caducidad de la clave, a elección del consumidor ;)
- Punto Importante. Tenemos que introducir nuestros datos, es útil que pongamos la dirección de correo que estemos usando en el mutt.
- Una vez validados los datos nos pide una clave secreta, lo de siempre, que no sea muy fácil, que mezcle números y letras, que alterne mayúsculas y minúsculas, etc... Un consejo, que no sea muy larga ya que tendremos que teclearla bastantes veces (8 carácteres estaría bien)
- Ahora en nuestro directorio $HOME/.gnupg disponemos de nuestras claves. **pubring.gpg** es la clave publica y que debemos distribir al mundo para que nos conozcan ;) y **secring.gpg** que es nuestra clave secreta que debemos ocultar de todo el mundo y de la que no viene nada mal hacer una copia de seguridad
- El siguiente paso es averiguar nuestro ID, para esto hacemos `gpg --list-key` y nos apuntamos el numerillo que aparece al lado de nuestro nombre (algo de la siguiente pinta
  `pub 1024D/`**`B41B382D`** `2001-12-13 Celso (PerroVerd)`
- Ahora editamos nuestro archivo .muttrc y añadimos la siguiente línea `set pgp_sign_as="0xB41B382D"` sustituyendo el numerillo por el que tengamos nosotros (nota el 0x del principio es necesario)

Con esto ya tenemos GPG funcionando en nuestra máquina, ahora veamos las cosas que podemos hacer con GPG

Firmar mensajes

Escribimos el mensaje y en la misma pantalla donde vamos a dar enviar debemos ver **PGP: En claro**, pulsamos la tecla 'p', con esto nos aparecen opciones para decidir que queremos hacer con el mensaje, en nuestro caso firmarlo (tecla 'i'), ahora veremos en la pantalla **PGP: Firmar** y además **firmar como: 0xB41B382D**. Ahora enviamos el mensaje y nos pedirá nuestra clave de GPG, la metemos y listos

Cifrar un mensaje

Lo primero que necesitamos para cifrar un mensaje es la clave pública de la persona a la que queremos enviar el mensaje, podemos pedirsela al personaje por correo, en mano, a través de su página web o de algun servidor de claves. Para añadir la clave a nuestro anillo hacemos
`gpg --import nombre_del_fichero_con_la_clave` desde una consola.
Una vez en mutt escribimos el mensaje y antes de enviar pulsamos la tecla 'p' y seleccionamos la opci¢n cifrar (letra 'd') o bien cifrar y firmar a la vez (letra 'o'), nos pide la clave y listos

Enviar una clave pública por email

Es tan sencillo como pulsar Escape y 'k'. Escribir el destinatario del correo y después seleccionar la clave que queremos enviar (si lo dejamos en blanco nos muestra todas las de nuestro anillo)

Lista de enlaces de este artículo:

1. http://rpmfind.net/linux/rpm2html/search.php?query=gnupg&submit=

E-mail del autor: celso _ARROBA_ mitago.net