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

PGP/MIME(Ägypten) en KMail - COMO (18218 lectures)

Per **Eduard Llull**, ***Daneel*** ()

Creado el 17/02/2003 09:42 modificado el 25/05/2003 17:59

Desde hace unos días, la distribución Debian[1] Sid ya incluye los paquetes del escritorio KDE[2], versión 3.1 (a día de hoy todavía faltan algunos). Una de las mejoras[3] en esta versión es la posibilidad de utilizar PGP/MIME en el gestor de correos KMail[4].
De momento no es algo sencillo configurar nuestro sistema para que haga uso de esta característica, pero espero que mi esfuerzo sirva para ponérselo más sencillo a los demás.

Actualización (21/02/2003)[5]:
Cómo hacer que KMail utilice PGP/MIME por defecto.

Actualización (27/03/2003):
Actualizado el paquete gpgsm de mi repositorio[6] debido a la actualización de la libreria libpth2 en Debian Sid.

Actualización (25/05/2003):
Actualizado el paquete gpgsm resolviendo el bug que causaba un *Segmentation Fault* al ejecutar el `gpg-agent`.
Ya no hace falta modificar el ficher `/etc/kde3/kdm/Xsession` para que se ejecute el agente[7] al arrancar el gestor de ventanas.

Igual te estaras preguntando cuál es el beneficio de utilizar PGP/MIME en lugar del "PGP-Inline". Primero veamos de forma muy simple como funciona el GnuPG[8]: cuando escribimos un correo y lo firmamos o ciframos, se crea un bloque GPG que está dentro del cuerpo del mensaje.
Pero, ¿qué pasa si el correo tiene adjuntos? Pues al estar fuera del cuerpo del mensaje no se utilizan para calcular la firma y no son cifrados por lo que lo único que va protegido es el cuerpo del mensaje Sin embargo, el PGP/MIME permite firmar/cifrar correos con adjuntos dándonos una mayor seguridad. Aquí residen los beneficios del PGP/MIME.

Bueno, ya es hora de ponernos a trabajar. Como ya es sabido, de momento no hay paquetes deb oficiales de KMail (entre otras aplicaciones pertenecientes a kdenetwork). Para poder instalar esta aplicación debemos incluir en nuestro `source.list`, además de los repositorios oficiales de Debian Sid, las líneas [gracias a Ricardo Galli por la lista]:

```
 deb http://people.debian.org/~ccheney/kde-other/ ./
deb http://people.debian.org/~ccheney/kde-3.1.0-1/ ./
deb http://people.debian.org/~bab/kde3.1/ ./
```

Actualización:esto ya no es cierto (aunque lo fue cuando se redactó el artículo 8-) así que podemos instalar las KDE y el KMail usando los repositorios oficiales de Debian Sid.

Con esto ya podremos instalar el KMail. Como queremos poder firmar/cifrar mensajes, también deberemos instalar GnuPG: `apt-get install kmail gnupg`. Con esto ya podremos firmar/cifrar los mails usando GPG-Inline. Bueno, realmente faltaría crear el par de claves (pública/privada), pero H y Perroverd ya han escrito articulos sobre el tema (1[9] y 2[10]).

Ahora nos centraremos en los pasos que debemos seguir para poder usar el PGP/MIME. Como podemos leer en el HOWTO oficial[11], el soporte PGP/MIME de KMail se realiza a través de un *plug-in* externo creado por Äegypten[12]. Para que funcione dicho *plug-in* necesitamos los siguientes programas y librerías

- libgcrypt (>= 1.1.10)
- gpgme 0.3.x (>.3.14; <= 0.4.0)
- cryptplug 0.3.x (>= 0.3.15)
- pinentry (>= 0.6.8)

Algunas de las librerías están disponibles oficialmente en forma de paquetes deb para Sid, pero otras no. En ftp://ftp.gnupg.org/gcrypt/alpha/aegypten/debian[13] se pueden encontrar los paquetes que faltan, pero las versiones no son correctas. Para facilitar las cosas a todos los Debianitas que quieran usar PGP/MIME he creado los paquetes necesarios, basándome en los desfasados que se pueden encontrar en el FTP anteriormente mencionado. Para poder instalarlos, debéis añadir a vuestros `sources.list` mi repositorio de paquetes: `deb http://bulma.net/~daneel/debian/ ./`

Entonces, ahora podemos instalar los paquetes necesarios: `apt-get install libgcrypt7 libgpgme11 cryptplug pinentry-qt`

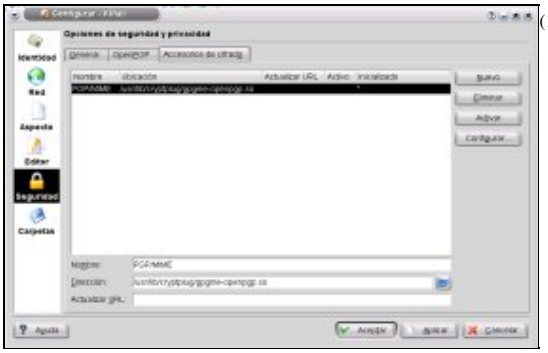
Una vez instalados estos paquetes debemos modificar unas cuantas cosillas:

1. Añadir 'use-agent' al fichero `~/.gnupg/options`
2. Crear el fichero ~/.gnupg/gpg-agent.conf con las siguientes líneas:

```
pinentry-program /usr/bin/pinentry-qt
no-grab
default-cache-ttl 1800
```

3. Debemos hacer que al entrar en las KDE, se ejecute el comando `eval "$(gpg-agent --daemon)"`. Yo he probado de añadir la línea al fichero `~/.Xsession` pero no se me ejecuta (inicio la sesión desde KDM). Añadir un script dentro de `~/.kde/Autostart/` tampoco ha dado resultados. Lo único que me ha ido bien ha sido modificar el fichero `/etc/kde3/kdm/Xsession` para que incluya el comando. No me acaba de gustar esta solución, pero de momento funciona.
   Actualización: Si se utiliza el paquete de mi repositorio, este último punto ya no hace falta. A partir de la versión 0.9.4-4 del paquete gpgsm, se instala un script en `/etc/X11/Xsession.d` que se encarga de arrancar el `gpg-agent`.

Para acabar, debemos configurar el KMail. En el menú, iremos a *Preferencias* -> *Configurar KMail* -> *Seguridad* -> *Accesorios de cifrado*. Pulsaremos el botón *Nuevo* y en los campos de la parte inferior del diálogo pondremos como **Nombre** `PGP/MIME` y en el campo **Dirección**, `/usr/lib/cryptplug/gpgme-openpgp.so`.


(14)

Ahora, al escribir un correo que queramos firmar/cifrar, podemos elegir en un desplegable de la barra de herramientas el sistema de criptografía (GnuPG o PGP/MIME) que queremos usar.

Actualización: si queremos que por defecto KMail utilice PGP/MIME, debemos pulsar el botón 'Activar' en el dialogo en el que hemos configurado el *plug-in*, teniendo seleccionado la línea correspondiente.

NOTA: a mi me pasa algo un poco extraño, el dialogo para la introducción de la *passphrase* de nuestra clave se me cierra automáticamente pasados unos 15 segundos. No se a que es debido, ni si es una *feature*, pero me pasa 8-)

Espero que este artículo junto a todos los que tenemos en esta web sobre GPG (ver caja de relacionados de la columna derecha) anime a la gente a proteger sus correos. Lo he escrito como un resumen de lo que he hecho yo para que funcionara en mi sistema, así que puede ser que haya hecho algo que no esté escrito. Pero si alguien tiene problemas instalando el PGP/MIME le recomiendo, primero, que lea el HOWTO oficial[11] y si todavía sigue sin funcionarle, que escriba un comentario a este artículo.

Lista de enlaces de este artículo:

1. http://www.debian.org/
2. http://www.kde.org/
3. http://promo.kde.org/3.1/feature_guide.php
4. http://kmail.kdr.org
5. http://bulma.net/body.phtml?nIdNoticia=1692#update01
6. http://bulma.net/body.phtml?nIdNoticia=1692#repository
7. http://bulma.net/body.phtml?nIdNoticia=1692#startup
8. http://www.gnupg.org/
9. http://bulma.net/body.phtml?nIdNoticia=1684
10. http://bulma.net/body.phtml?nIdNoticia=1483
11. http://kmail.kde.org/kmail-pgpmime-howto.html
12. http://www.gnupg.org/aegypten/
13. ftp://ftp.gnupg.org/gcrypt/alpha/aegypten/debian
14. http://bulma.net/~daneel/webbulma/kmail-pgpmime-plugin-config.png

---

E-mail del autor: daneel _ARROBA_ bulma.net
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1692