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

GPG. Preguntas y respuestas rápidas (19070 lectures)

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

Creado el 06/09/2002 19:02 modificado el 06/09/2002 19:02

Este artículo pretende ser una chuleta rápida en la que podemos encontrar las cosas que son necesarias para una gestión de claves eficaz en gpg.

¿Como envio mi clave a un servidor?

Tengo que configurar un servidor de claves en .gnupg/options basta con añadir la opción keyserver pgp.rediris.es (por ejemplo) y ejecutar gpg --send-keys mi_clave

¿Como bajo una clave de un servidor?

Una vez configurado el keyserver basta con hacer un gpg --search-key una_clave o bien un gpg --recv-keys una_clave

¿Como compruebo el fingerprint de una clave?

Se emplea gpg --fingerprint una_clave y para comprobarlo no te queda más remedio que hacerlo a mano mirando si el fingerprint de nuestro ordenador corresponde con el que nos han dado

¿Cómo firmo una clave?

Usamos gpg --edit-key una_clave, nos presenta una pantalla en la que podemos introducir ordenes, usaremos la orden sign y después de confirmar que queremos firmar haremos un save

He visto un fingerprint en un correo que me ha llegado, lo he comprobado y es correcto ¿Puedo firmar esa clave?

NO, no y no. El hecho de firmar una clave no significa que la clave sea correcta, implica que la persona propietaria de la firma es quien dice ser. Eso solo lo podemos conseguir intercambiando claves en persona y comprobando las identificaciones personales de las personas a las que firmamos

He firmado una clave ¿Qué hago ahora?

Lo ideal sería enviar esa firma a un servidor de claves. Para esto haremos gpg --send-key clave_firmada. Ojo, clave_firmada es el identificador de la clave que hemos firmado, NO es nuestra clave.

¿Cómo añado una dirección más de correo a mi clave?

Tenemos que editar nuestra clave, para eso hacemos gpg --edit-key nuestra_clave, y en las ordenes ponemos adduid, introducimos los datos que nos pide y hacemos save. Ademas nos conviene volver a enviar la clave al servidor

¿Qué mantenimiento requiere el anillo?

Dos cosas:

- Mantener actualizados los niveles de confianza (ya hablaremos de ellos otro día con Anacleto y Biturcio) con la orden gpg --check-trustdb (automatica) o gpg --update-trustb (manual). Yo utilizo el check a través del cron
- Refrescar las actualizaciones de las claves del servidor. Nos interesa saber si alguién añade una firma a una clave y la

envia a un servidor. Para esto hacemos un gpg --refresh-keys que se encarga de comprobar si una clave de un servidor ha sido modificada y en caso afirmativo descarga las actualizaciones. Otra tarea candidata para el cron

---

E-mail del autor: celso _ARROBA_ mitago.net