

Title: Uso de gpg Date: 2015-11-28 09:51 Modified: 2015-11-28 09:51 Category: Linux Tags: linux, gpg Slug: usos_gpg
Authors: procamora Summary:

##Creación de un nuevo key-pair #####Generaremos nuestra pareja de llaves (pública y privada), que posteriormente utilizaremos para la encriptación de ficheros, utilizaremos el siguiente comando: `sudo gpg --gen-key`

##Importar y exportar keys #####Tras crear nuestra llave, podemos importarla o exportarla en distintos equipos, desde los que tenemos intención de compartir ficheros encriptados, para importar una llave ejecutamos: `sudo gpg --import Public-key.asc`

#####Podemos exportar nuestra key del siguiente modo (ascii), luego podríamos utilizar el comando anterior para importarla en otro equipo. -ascii crea una salida ascii con armadura.: `sudo gpg --armor --export UID > Public-key.asc`

#####Una vez importada la key en nuestro sistema, conviene firmarla para verificar la veracidad de la llave, utilizaremos el siguiente comando, donde UID es el ID/nombre de la llave.: `sudo gpg --sign-key 'UID'`

#####para exportar clave privada: `sudo gpg --armor --export-secret-key UID > Private-key.asc`

##Encriptar y desencriptar #####Una vez que tenemos la llave creada, instalada y firmada en el sistema, ya podemos empezar a encriptar y desencriptar ficheros. En el siguiente ejemplo vamos a encriptar un fichero de texto, los parámetros indican que se firma y cifra (-ser) para el usuario con su determinado UID/nombre creando una salida ascii con armadura (-a). tendremos que escribir la frase contraseña de la llave para hacer efectivo el cifrado: `sudo gpg -s -a -u 'UID' test2.txt`

Necesita una frase contraseña para desbloquear la clave secreta del usuario. "xxxx xxxx (xxx xxx)" clave DSA de 2048 bits, ID 7EEECF36, creada el 2010-11-08:

gpg el agente gpg no esta disponible en esta sesión Introduzca frase contraseña:

#####Para hacer el proceso inverso de descifrado, utilizaríamos el siguiente comando, donde -d indica desencriptar y mensaje-cifrado.asc es el fichero generado en el anterior comando, que guardaremos en salida.txt: `sudo gpg --output salida.txt -d mensaje-cifrado.asc`

El proceso de desencriptar ficheros de equipos remotos es el mismo siempre que haya sido encriptado utilizando tu misma llave pública.:

La gestión básica de llaves resumiría los siguientes comandos:

#####Listar las llaves instaladas en el sistema: `sudo gpg --list-keys`

#####Borrar llave "test@test.com" instalada en nuestro sistema: `sudo gpg --delete-key 'test@test.com'`