# EJERCICIO CON GPG

El caso de estudio del área de Recursos Humanos, Pedro requiere mandar el archivo de seguimiento de evaluación de su personal a la jefa Julia de Recursos Humanos garantizando la autenticidad, confidencialidad y no repudio, para ello se crean sus llaves privadas y públicas.

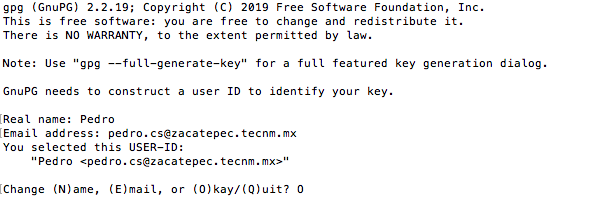
|  |  |
| --- | --- |
| Profesor | Programador |
| Pedro  (Jefe del CI) | Julia  (Jefa de RH) |

CREAR PAR DE LLAVES PÚBLICA Y PRIVADA PARA PEDRO

$gpg –gen-key



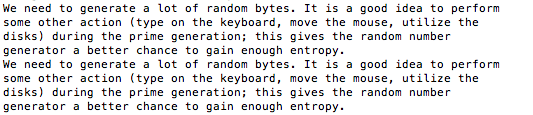
Datos necesarios y confirmando:



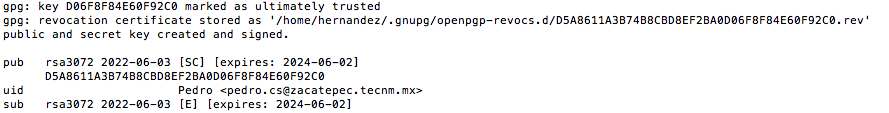
Contraseña privada (**pedro1234567890.**)

|  |  |
| --- | --- |
|  |  |

Generación de entropía



Creación exitosa

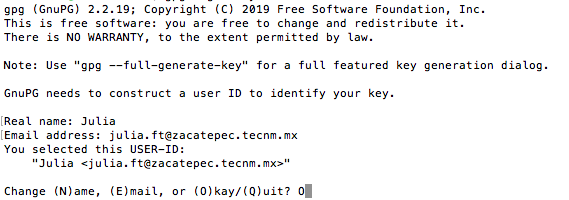


CREAR PAR DE LLAVES PÚBLICA Y PRIVADA PARA JULIA

$gpg –gen-key



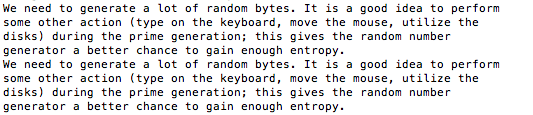
Datos necesarios y confirmando



Se solicita la contraseña (**julia1234567890.**)

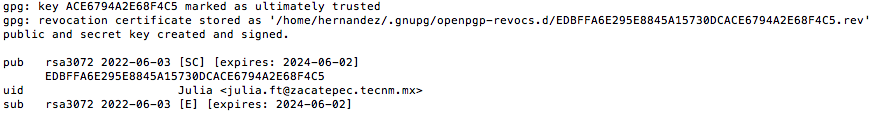
|  |  |
| --- | --- |
|  |  |

Generación de entropía



©

Creación exitosa



EXPORTAR UNA LLAVE PÚBLICA EN FORMATO ASCII

$gpg -a --export id\_llave > archivo.pub

Se exportan ambas llaves pública

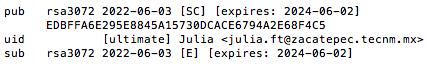




Se enlistan las llaves



Información del usuario Julia



Información del usuario Pedro



IMPORTAR LLAVE PÚBLICA

Se tiene que importar la llave pública a la autoridad, para ello se hace la copia del archivo julia.pub y pedro.pub a la carpeta /INTERNET/

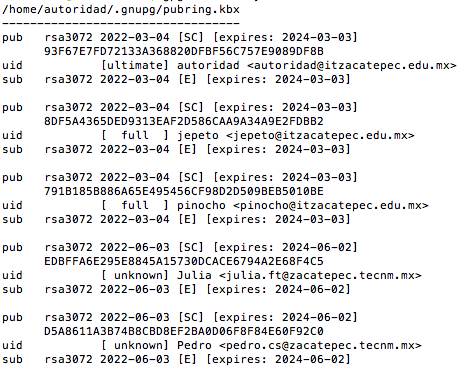


Para importar una llave pública, puede ser una o varias



Se enlista las llaves



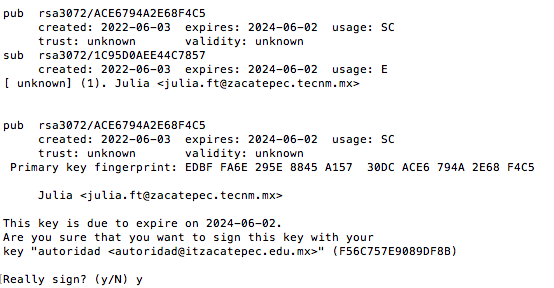


PARA FIRMAR UNA LLAVE PÚBLICA

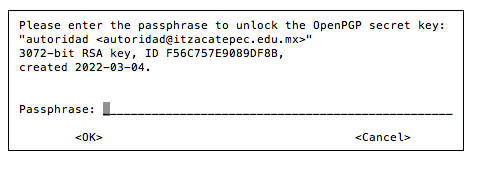
Para el usuario Julia



Se hace la pregunta, realmente quiere firmar.



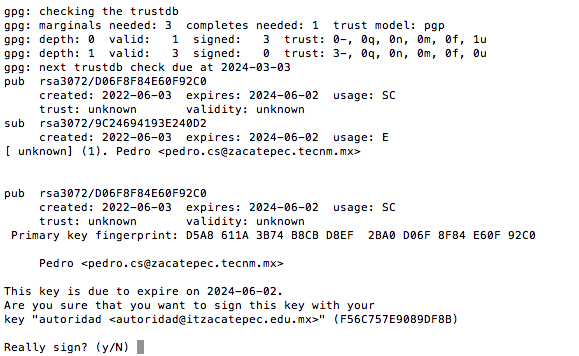
Se pide la contraseña de la autoridad



Se aplica la firma de la llave pública para el usuario Pedro



Se hace la pregunta, realmente quiere firmar.

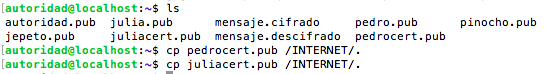


Como ya fue firmado por la AUTORIDAD es necesario exportar las llaves publicas

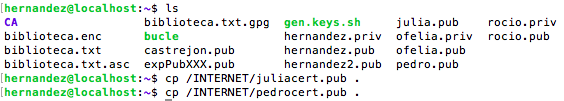




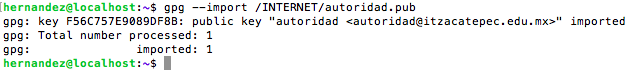
Se verifica que se encuentren los archivos y posteriormente se hace nuevamente la copia a la carpeta general /INTERNET/

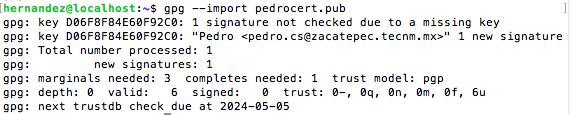


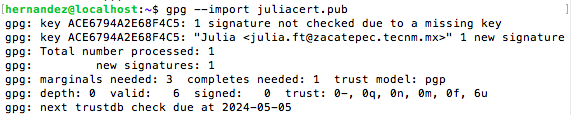
Se vuelve a la sesión de usuario y se hace la copia de los archivos pedrocert.pub y juliacert.pub



Se importan las llaves firmadas por la autoridad y tambien la autoridad

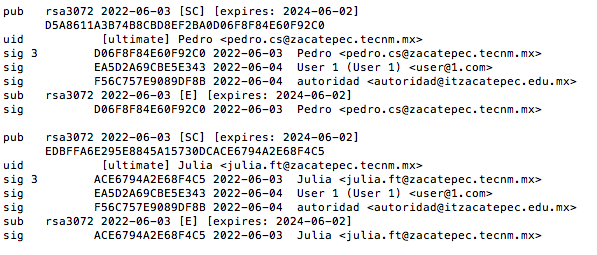






Se hace el listado





PARA MANDAR EL ARCHIVO

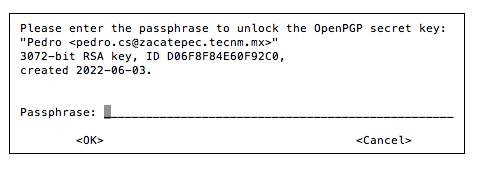
Se genera un archivo de prueba – biblioteca.txt



Posteriormente se cifra el archivo



Se solicita la contraseña



Descrifra el archivobib



Práctica en un equipo de Linux con instalación del openGPG y la herramienta de generación de entropía

|  |  |  |
| --- | --- | --- |
| Profesor | Profesor | Programador |
| Pinocho | Jepeto | autoridad |

Desde la cuenta del administrador

1. Se crearon los usuarios con contraseña 123456

#add pinocho

#add jepeto

#add autoridad

Desde la sesión de cuenta de pinocho

1. Se crearon su par de llaves

$gpg --ken-key

// datos necesarios (nombre y correo)

// se confirma los datos

//se genera entropía

//crea una carpeta /home/pinocho/.gnupg/opengpg -revocs.d

// /home/pinocho/.gnupg/trustdb.gpg

//crea carpeta de revocación /home/pinocho/.gnupg/opengpg-revocs.d/xxxxxx.rev

//contraseña 123456

//pub rsa3072 2022-03-04[SC] [expires:2024-03-03]

1. Se exporta la llave pública

$gpg -a--export [pinocho@itzacatepec.edu.mx](mailto:pinocho@itzacatepec.edu.mx) > pinocho.pub

1. Se hace la copia a una carpte de raiz /INTERNET/

$cp pinocho.pub /INTERNET/.

Desde la sesión de cuenta de jepeto

1. Se crearon su par de llaves

$gpg --ken-key

// datos necesarios (nombre y correo)

// se confirma los datos

//se genera entropía

//crea una carpeta /home/jepeto/.gnupg/opengpg -revocs.d

// /home/jepeto/.gnupg/trustdb.gpg

//crea carpeta de revocación /home/jepeto/.gnupg/opengpg-revocs.d/xxxxxx.rev

//contraseña 123456

//pub rsa3072 2022-03-04[SC] [expires:2024-03-03]

1. Se exporta la llave pública

$gpg -a--export [jepeto@itzacatepec.edu.mx](mailto:jepeto@itzacatepec.edu.mx) > jepeto.pub

1. Se hace la copia a una carpte de raiz /INTERNET/

$cp pinocho.pub /INTERNET/.

Desde la cuenta de autoridad

1. Exporta su llave pública

$gpg -a--export [autoridad@itzacatepec.edu.mx](mailto:autoridad@itzacatepec.edu.mx) > autoridad.pub

1. Se hace la copia a una carpte de raiz /INTERNET/

$cp autoridad.pub /INTERNET/.

1. Hace la copia de las llaves públicas de pinocho y jepeto

$cp /INTERNET/pinocho.pub .

$cp /INTERNET/jepeto.pub .

1. Importa las llaves públicas

$gpg -a--import jepeto.pub pinocho.pub

1. Firma las llaves públicas y cada vez que firma le pide ingresar la contraseña

$gpg –sign-key [pinocho@itzacatepec.edu.mx](mailto:pinocho@itzacatepec.edu.mx)

$gpg –sign-key [jepeto@itzacatepec.edu.mx](mailto:jepeto@itzacatepec.edu.mx)

1. Exporta las llaves ya firmadas por la autoridad de pinocho y jepeto

$gpg -a--export [pinocho@itzacatepec.edu.mx](mailto:pinocho@itzacatepec.edu.mx) > pinocho2.pub

$gpg -a--export [jepeto@itzacatepec.edu.mx](mailto:jepeto@itzacatepec.edu.mx) > jepeto2.pub

1. Se hace la copia de las nuevas llaves publicas firmadas por la autoridad

$cp pinocho2.pub /INTERNET/pinocho.pub

$cp jepeto2.pub /INTERNET/jepeto.pub

Desde el usuario pinocho

1. Importamos la llave pública de pinocho, jepeto y autoridad

$gpg –import /INTERNET/pinocho.pub

$gpg –import /INTERNET/jepeto.pub

$gpg –import /INTERNET/autoridad.pub

1. Creamos un archivo con datos

$nano mensaje

1. Encriptamos y firmamos un archivo con salida en formato ASCCII

$gpg -u [pinocho@itzacatepec.edu.mx](mailto:pinocho@itzacatepec.edu.mx) -r [jepeto@itzacatepec.edu.mx](mailto:jepeto@itzacatepec.edu.mx) -sae -o mensaje.cifrado mensaje

1. Se hace la copia del mensaje cifrado para enviarselo a jepeto

$cp mensaje.cifrado /INTERNET/.

Desde el usuario jepeto

1. Importamos la llave pública de pinocho, jepeto y autoridad

$gpg –import /INTERNET/pinocho.pub

$gpg –import /INTERNET/jepeto.pub

$gpg –import /INTERNET/autoridad.pub

1. Se copia el mensaje cifrado que manda pinocho

$cp /INTERNET/ mensaje.cifrado .

1. desencriptamos el archivo

$gpg -u [jepeto@itzacatepec.edu.mx](mailto:jepeto@itzacatepec.edu.mx) -d mensaje.cifrado > mensaje

Cualquir usuario

Si un usuario X lo quisiera desencriptar no podría.