

IES Valle Inclán



Kleopatra y GPG en Linux

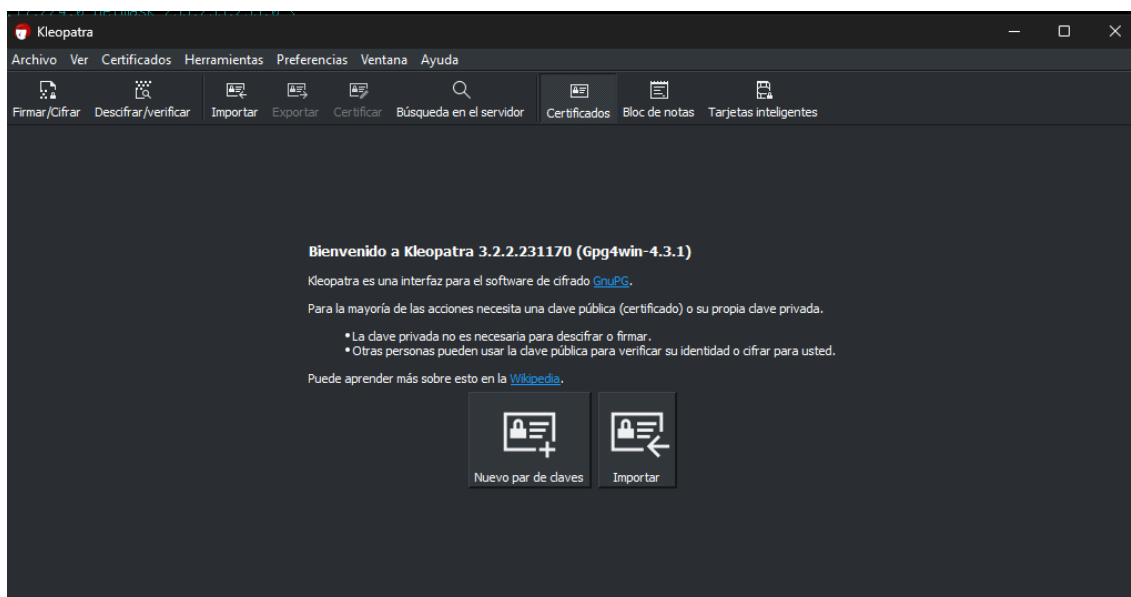
CARLOS GONZÁLEZ MARTÍN

Contenido

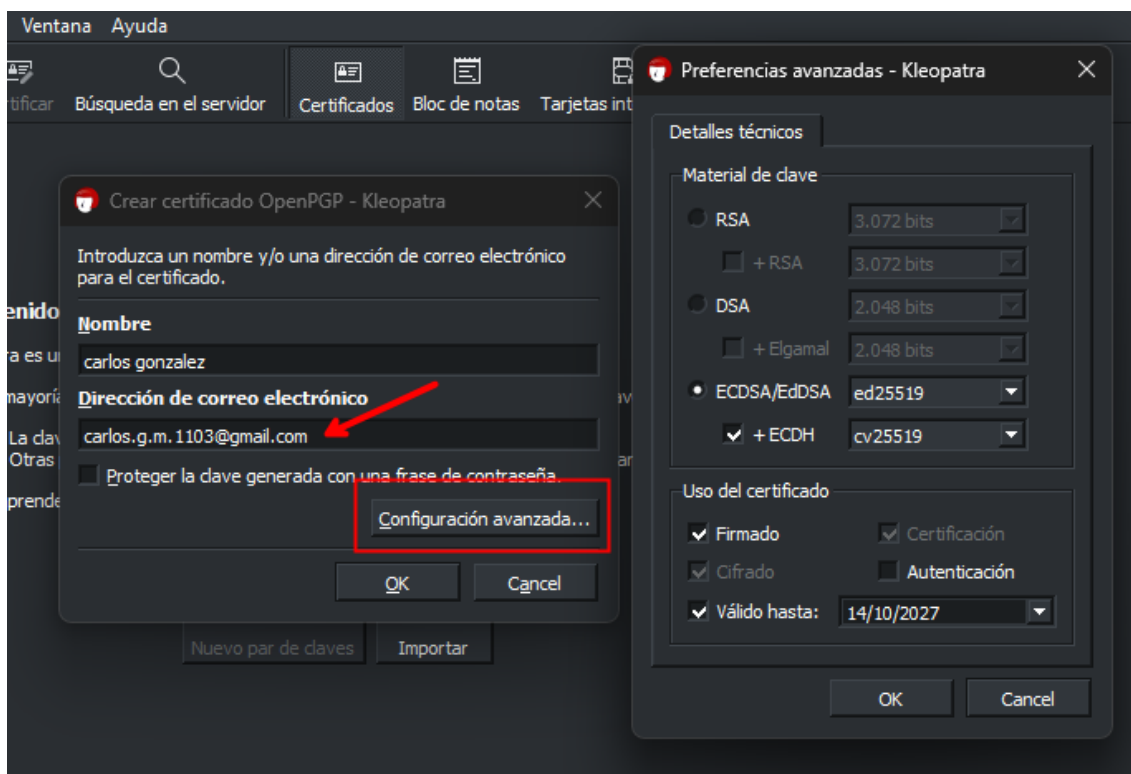
1.	Kleopatra.....	3
2.	Linux.....	9
3.	Conclusión	10

1. Kleopatra

Lo que haremos será descargar la herramienta y una vez instalada nos saldrá así.

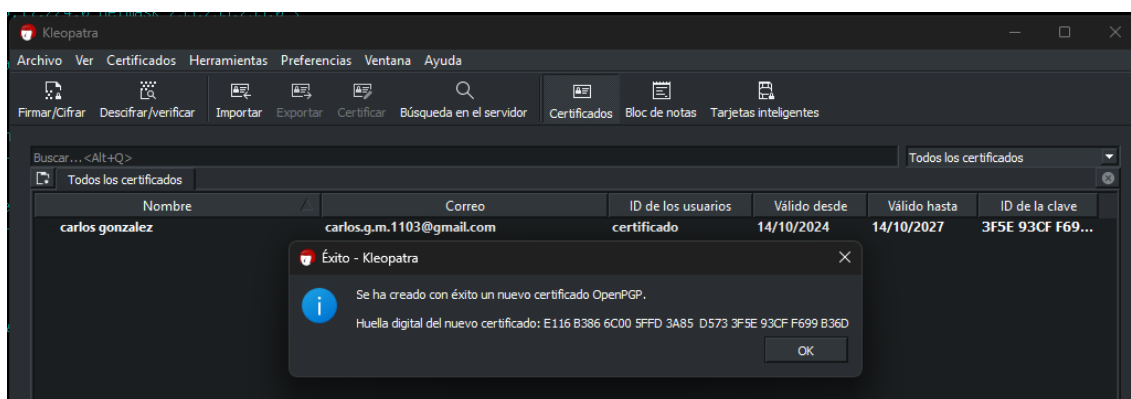


Una vez que estemos aquí le daremos a “nuevo par de claves” y crearemos el certificado.

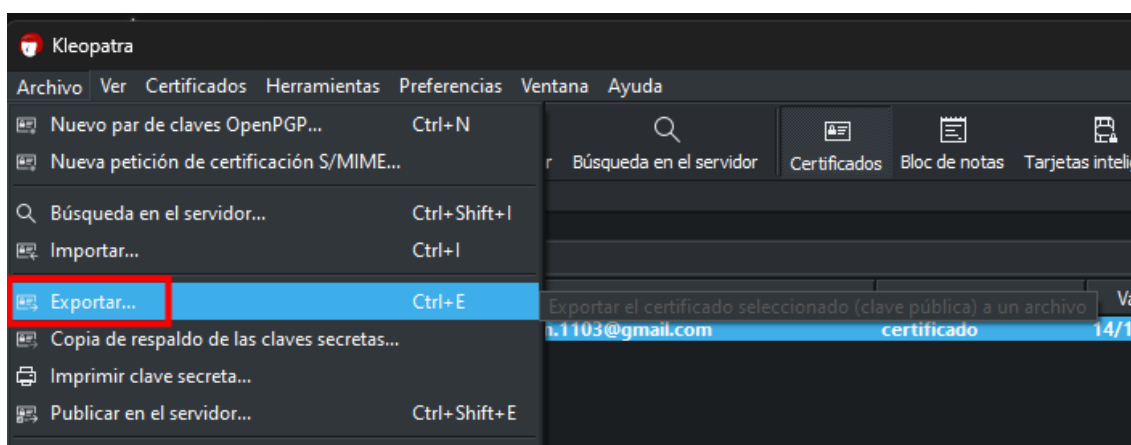


Una vez escrito el nombre y el correo electrónico, dándole a configuración avanzada veremos la validez del certificado.

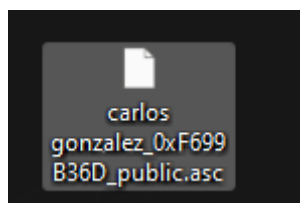
Una vez que le daremos a “ok” nos generara las claves correctamente.



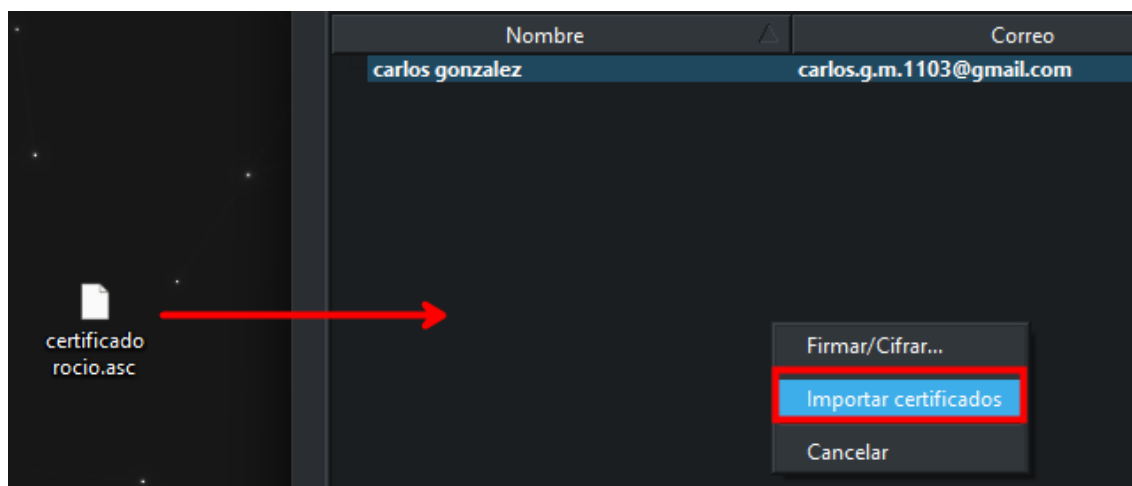
Una vez que esta creado el certificado le daremos a exportar.



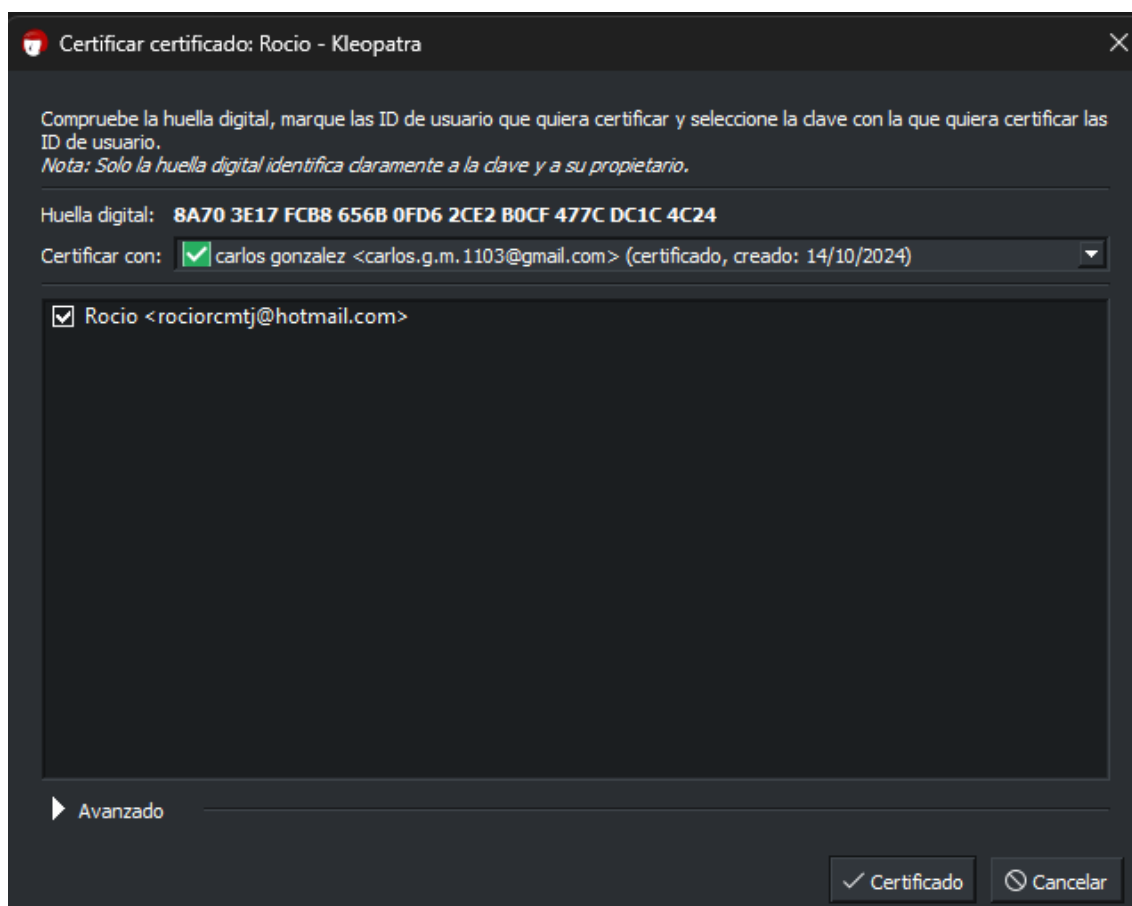
Una vez que le demos a exportar y lo guardaremos en el escritorio veremos el siguiente archivo.



Con otro certificado, por ejemplo, el de mi compi Rocío, le podremos dar a importar certificados cuando arrastremos el certificado.



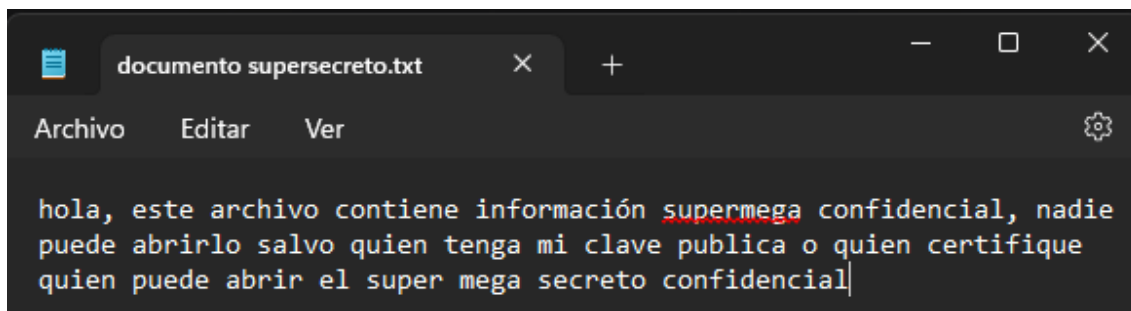
Una vez que le demos a importar certificados nos saldrá la siguiente ventana.



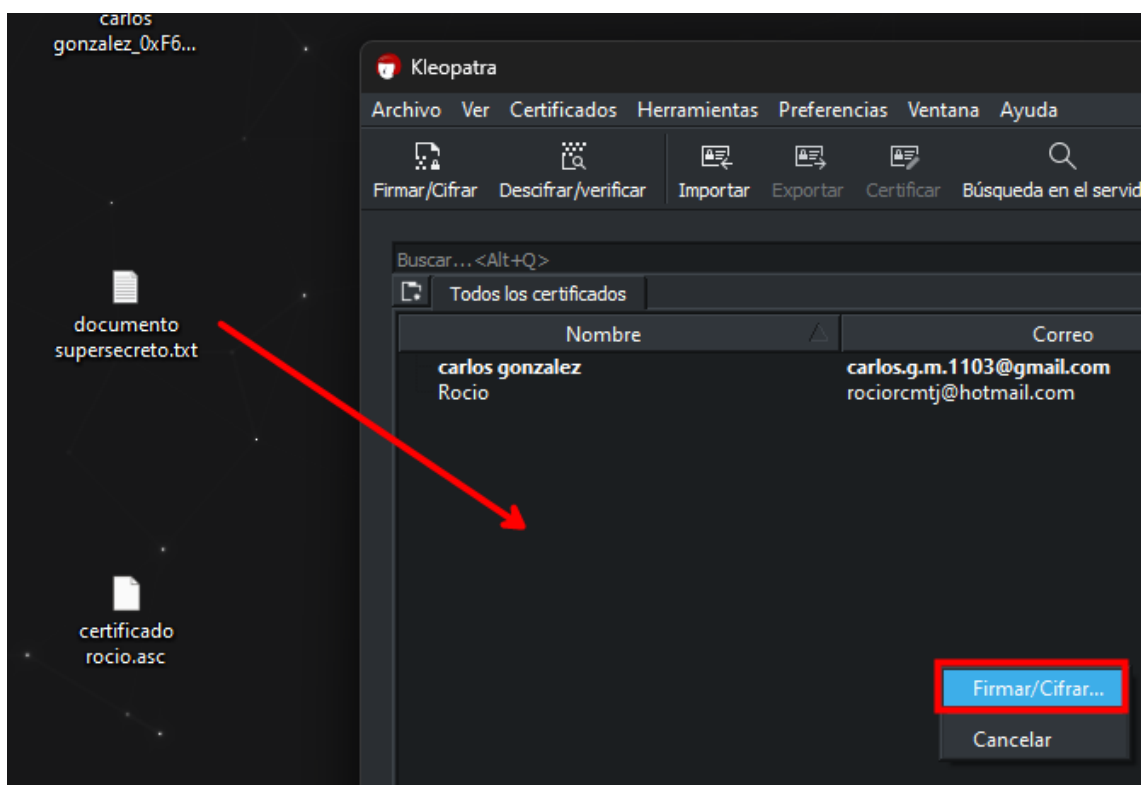
Y le daremos a “Certificado”.



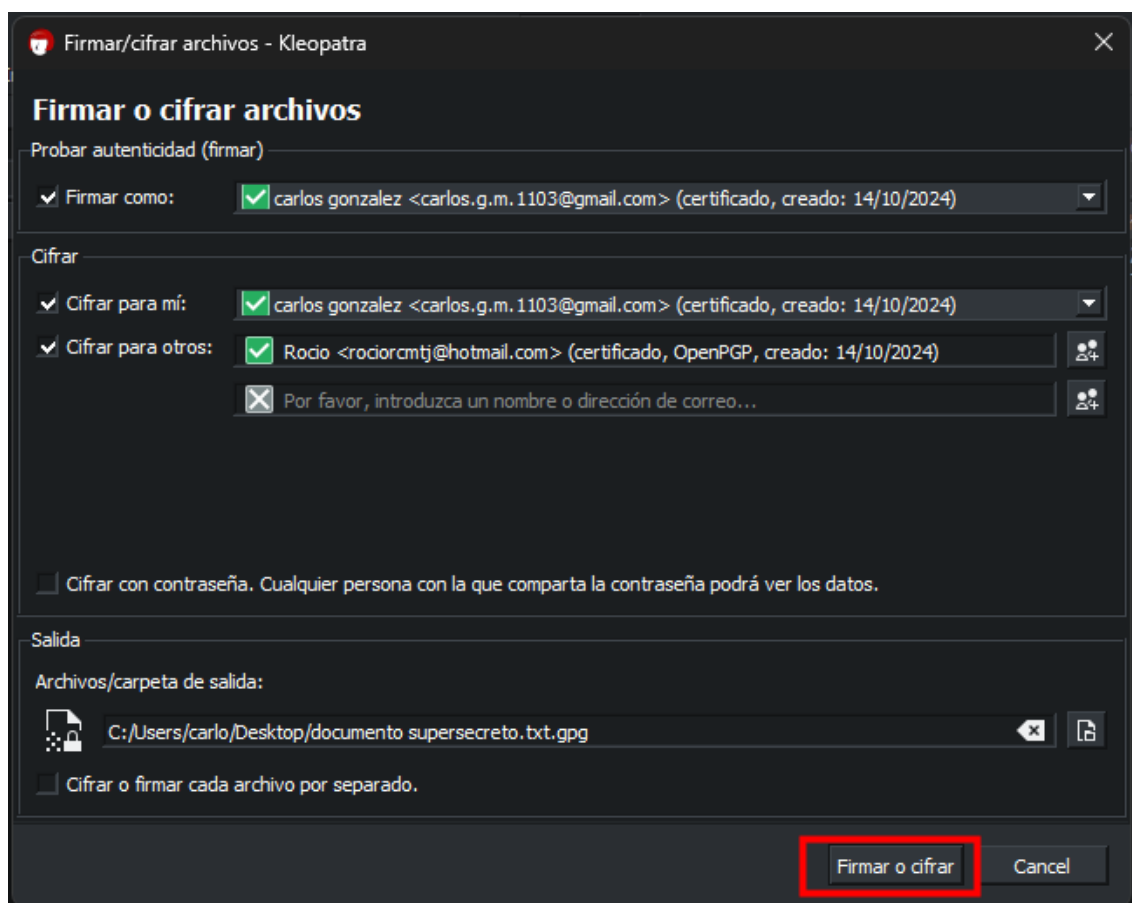
Una vez que tenemos los dos certificados procederemos a hacer un archivo llamado “documento supersecreto.txt”.



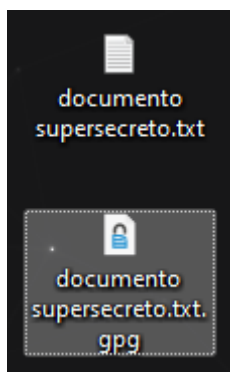
Una vez tenemos el documento guardado, lo que haremos será arrastrar el archivo a Kleopatra y le daremos a firmar/cifrar.



Una vez que le demos a firmar/cifrar nos saldrá la siguiente captura.

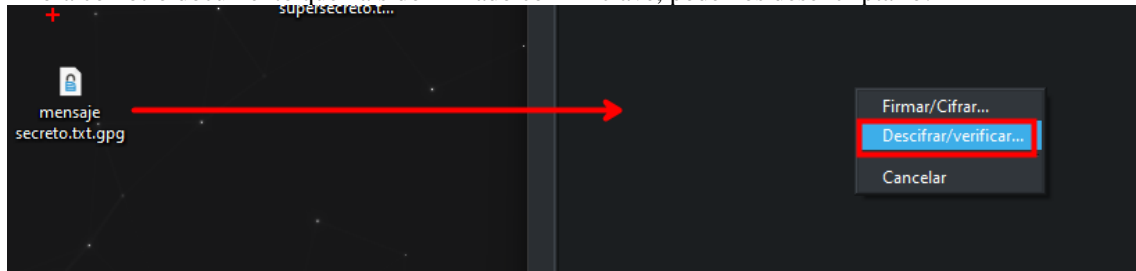


Le daremos a cifrar para otros y elegiremos el certificado que hemos importado anteriormente.

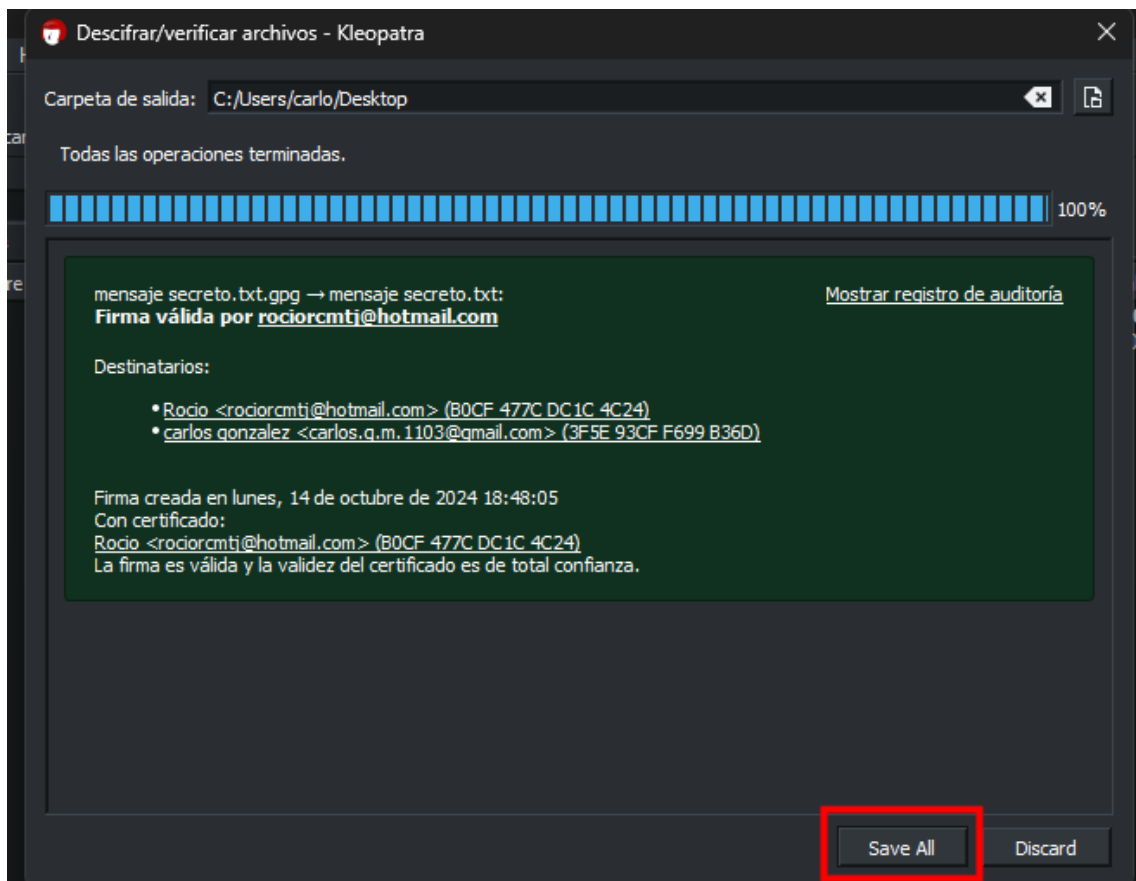


Una vez que le demos a firmar o cifrar nos saldrá el siguiente archivo.

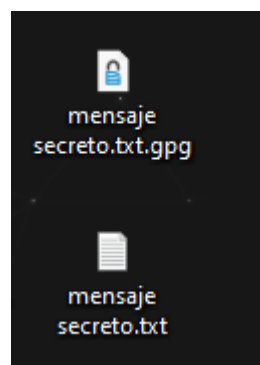
Ahora con otro documento que ha sido firmado con mi clave, podemos desenscriptarlo.

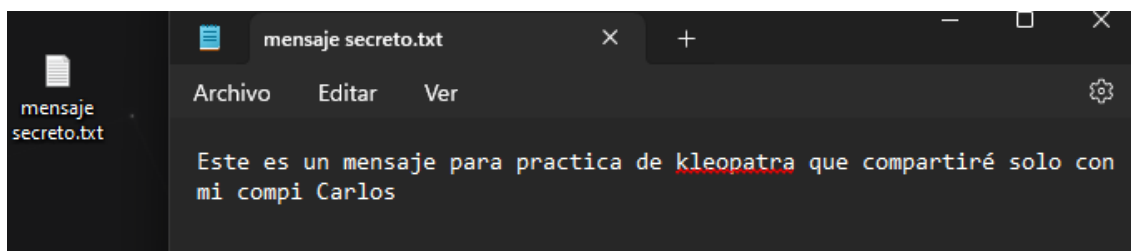


Una vez que le demos a descifrar/verificar nos saldrá la siguiente ventana y veremos que ha desenscriptado el archivo.



Una vez que le demos a “Save All”, nos saldrá el archivo descifrado.





Y como podemos comprobar podemos visualizar el contenido del archivo.

2. Linux

Por regla general el paquete “gpg” viene instalado, pero si no lo tenemos que usar el gestor de paquetes “apt”, y para instalarlo seria si estamos con Root “apt install gpg -y”, hay veces que tenemos que actualizar las librerías que seria con “apt update”. Pero si lo estamos usando con un usuario estándar del sistema témenos que usar al principio “sudo”.

Una vez instalado el paquete procederemos a instalar con el comando “gpg --gen-key”.

```
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: creado el directorio '/root/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/root/.gnupg/openpgp-revocs.d/8F86D461E09F983270F5D861B428B7DF9C9FE289.rev'
claves pública y secreta creadas y firmadas.

pub   rsa3072 2024-10-15 [SC] [caduca: 2026-10-15]
      8F86D461E09F983270F5D861B428B7DF9C9FE289
uid           carlos <carlos.g.m.1103@gmail.com>
sub   rsa3072 2024-10-15 [E] [caduca: 2026-10-15]

root@gpglinux:~# gpg --gen-key_
```

Una vez creada la exportaremos para que otro usuario del sistema la tenga.

```
root@gpglinux:~# gpg --export -a -o /tmp/claveroot.pub
root@gpglinux:~# ls -la /tmp/claveroot.pub
-rw-r--r-- 1 root root 2456 oct 15 11:56 /tmp/claveroot.pub
root@gpglinux:~#
```

Una vez que estamos con “usuario” importaremos la clave.

```
-rw-r--r-- 1 root root 2456 oct 15 11:56 /tmp/claveroot.pub
root@gpglinux:~# su usuario
usuario@gpglinux:/root$ cd
usuario@gpglinux:~$ gpg --import /tmp/claveroot.pub
gpg: creado el directorio '/home/usuario/.gnupg'
gpg: caja de claves '/home/usuario/.gnupg/pubring.kbx' creada
gpg: /home/usuario/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave B428B7DF9C9FE289: clave pública "carlos <carlos.g.m.1103@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg:      importadas: 1
usuario@gpglinux:~$
```

Ahora escribiremos un mensaje.

```
root@gpglinux:~# cat mensaje
hola, este es un mensaje super secreto que nadie puede tener salvo el quien pueda encriptar con mi clave publica
root@gpglinux:~#
```

Y encriptamos el mensaje.

```
usuario@gpglinux:~$ gpg -v -a -o mensaje.cifrado --encrypt --recipient carlos mensaje
gpg: usando pgp como modelo de confianza
gpg: usando subclave BBBD1A7231971439 en vez de clave primaria B428B7DF9C9FE289
gpg: BBBD1A7231971439: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra
sub rsa3072/BBBD1A7231971439 2024-10-15 carlos <carlos.g.m.1103@gmail.com>
Huella clave primaria: 8F86 D461 E09F 9832 70F5 D861 B428 B7DF 9C9F E289
Huella de subclave: B939 7494 7292 77BD 7A87 C3E4 BBBD 1A72 3197 1439
:
No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N) s
gpg: leyendo desde 'mensaje'
gpg: escribiendo en 'mensaje.cifrado'
gpg: RSA/AES256 cifrado para: "BBBD1A7231971439 carlos <carlos.g.m.1103@gmail.com>"
usuario@gpglinux:~$
```

Una vez encriptado con el otro usuario lo desencriptaremos.

```
Introduzca frase contraseña para desbloquear la clave secreta OpenPGP:
"carlos <carlos.g.m.1103@gmail.com>"
clave de 3072-bit RSA, ID BBBD1A7231971439,
creada el 2024-10-15 (ID de clave primaria B428B7DF9C9FE289).

Frase contraseña: *****
<OK> <Cancelar>

gpg: cifrado con clave de 3072 bits RSA, ID BBBD1A7231971439, creada el 2024-10-15
"carlos <carlos.g.m.1103@gmail.com>"
hola, este es un mensaje super secreto que nadie puede tener salvo el quien pueda encriptar con mi clave publica
root@gpglinux:/home/usuario# gpg --decrypt mensaje.cifrado
```

3. Conclusión

La parte de encriptación viene muy bien, ya que no sabes si el destinatario recibe completamente el mensaje o no y puede haber alguien escuchando la trama y alterándola, esto se usa mucho en las empresas, no con Kleopatra, que también se puede usar, pero hay versiones comerciales como SealPath, que lo cifra con tu nombre de usuario y solo lo puede descifrar el usuario que tu le indiques.