IES Valle Inclán

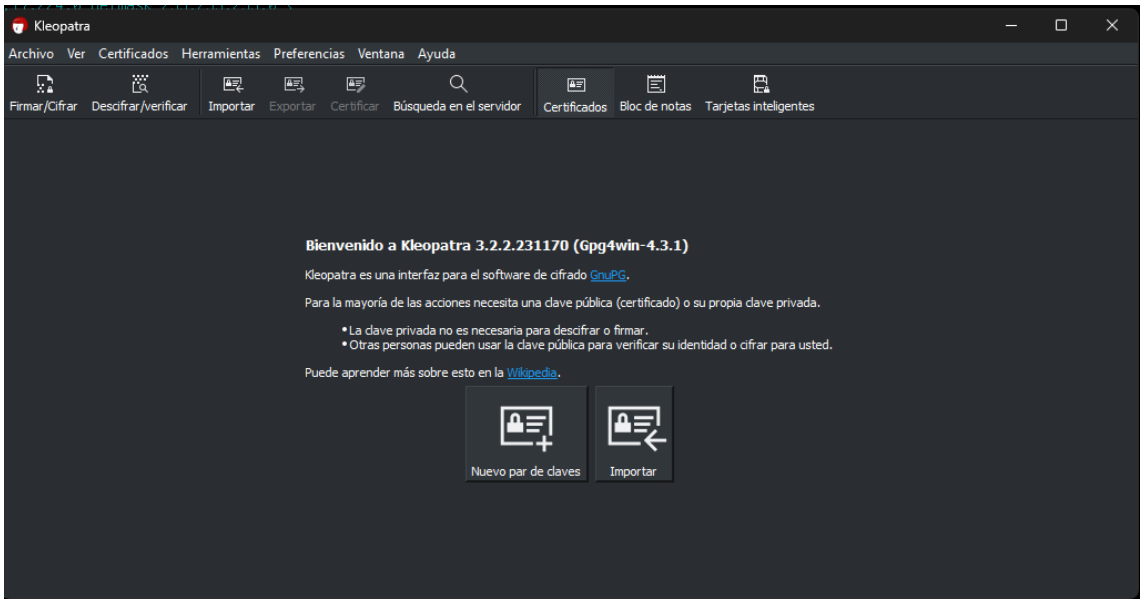
Kleopatra y GPG en Linux

CARLOS GONZÁLEZ MARTÍN

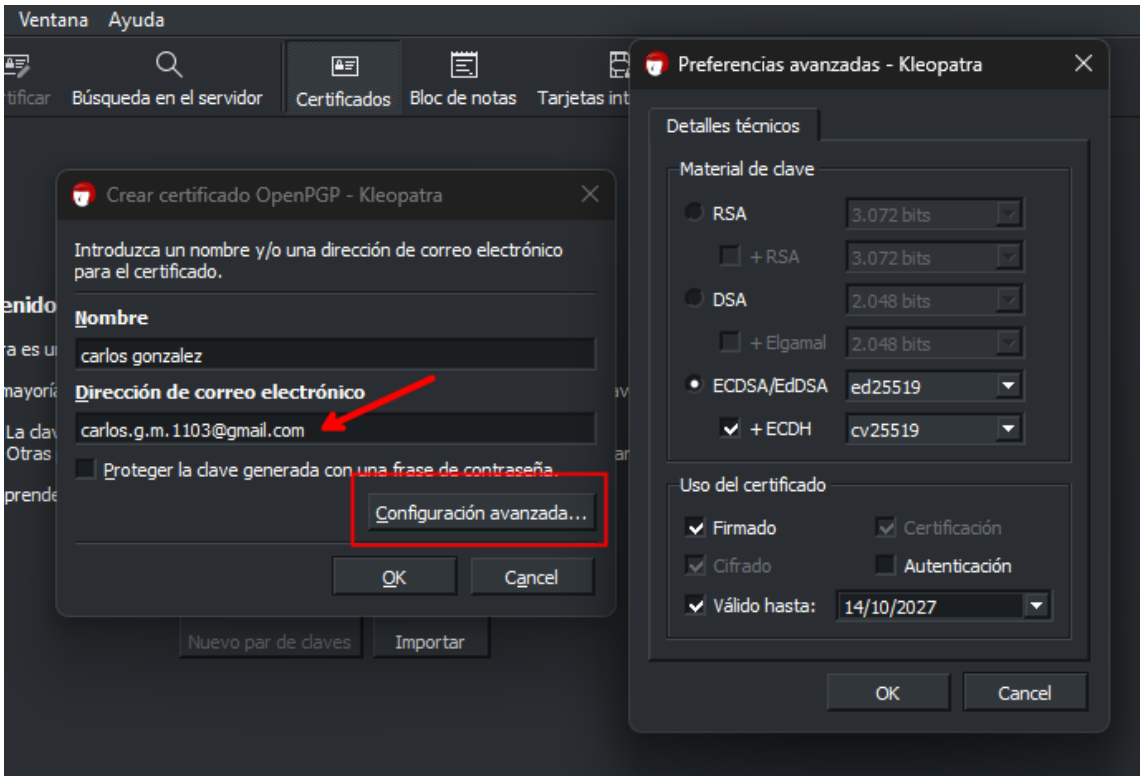
Contenido

1. Kleopatra

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

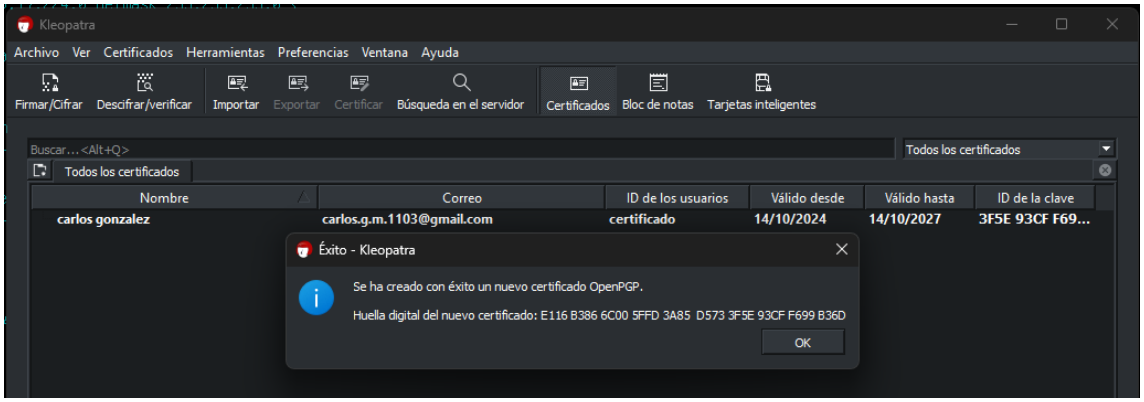


Una vez que estemos aquí le daremos a “nuevo par de claves” y crearemos el certificado.

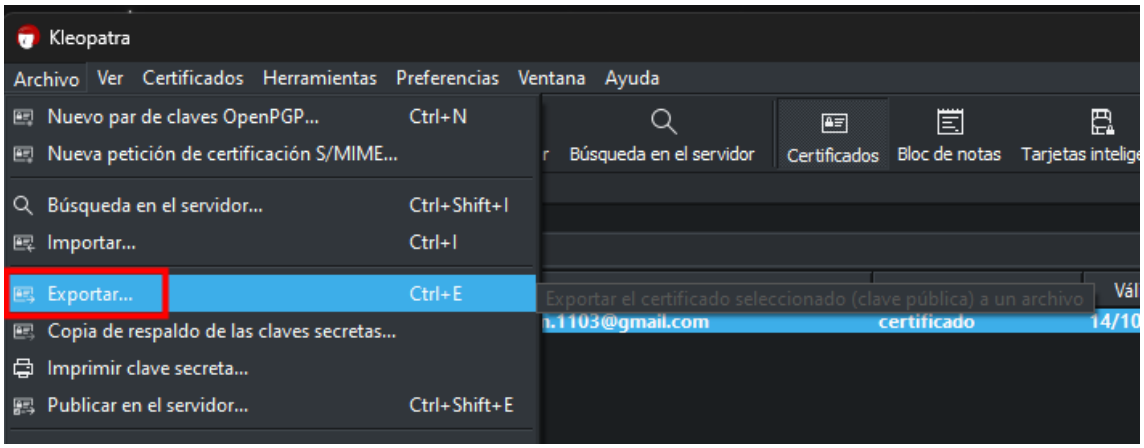


Una vez escrito el nombre y el correo electrónico, dándole a configuración avanzada veremos la validez del certificado.

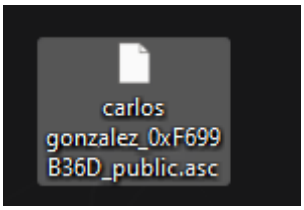
Una vez que le daremos a “ok” nos generara las claves correctamente.



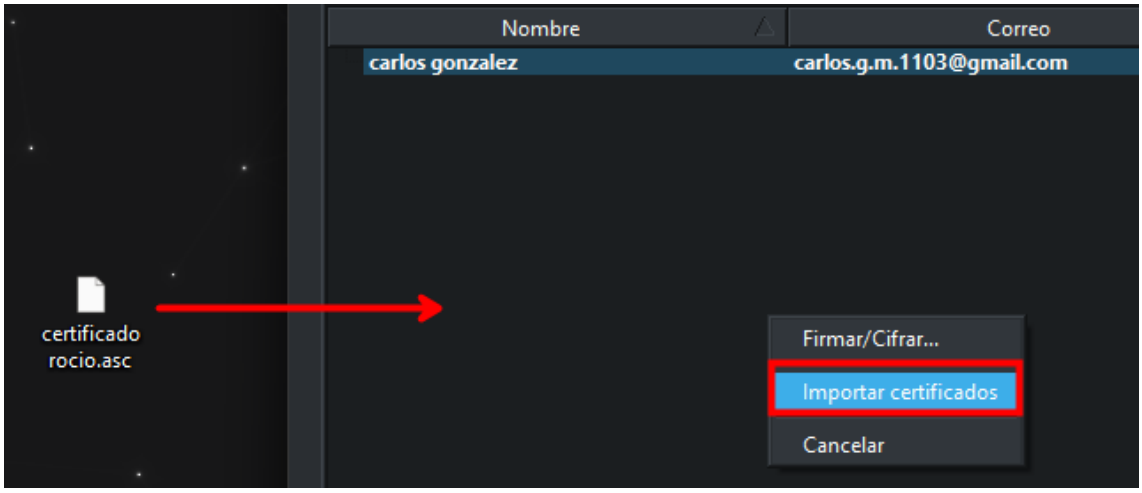
Una vez que esta creado el certificado le daremos a exportar.



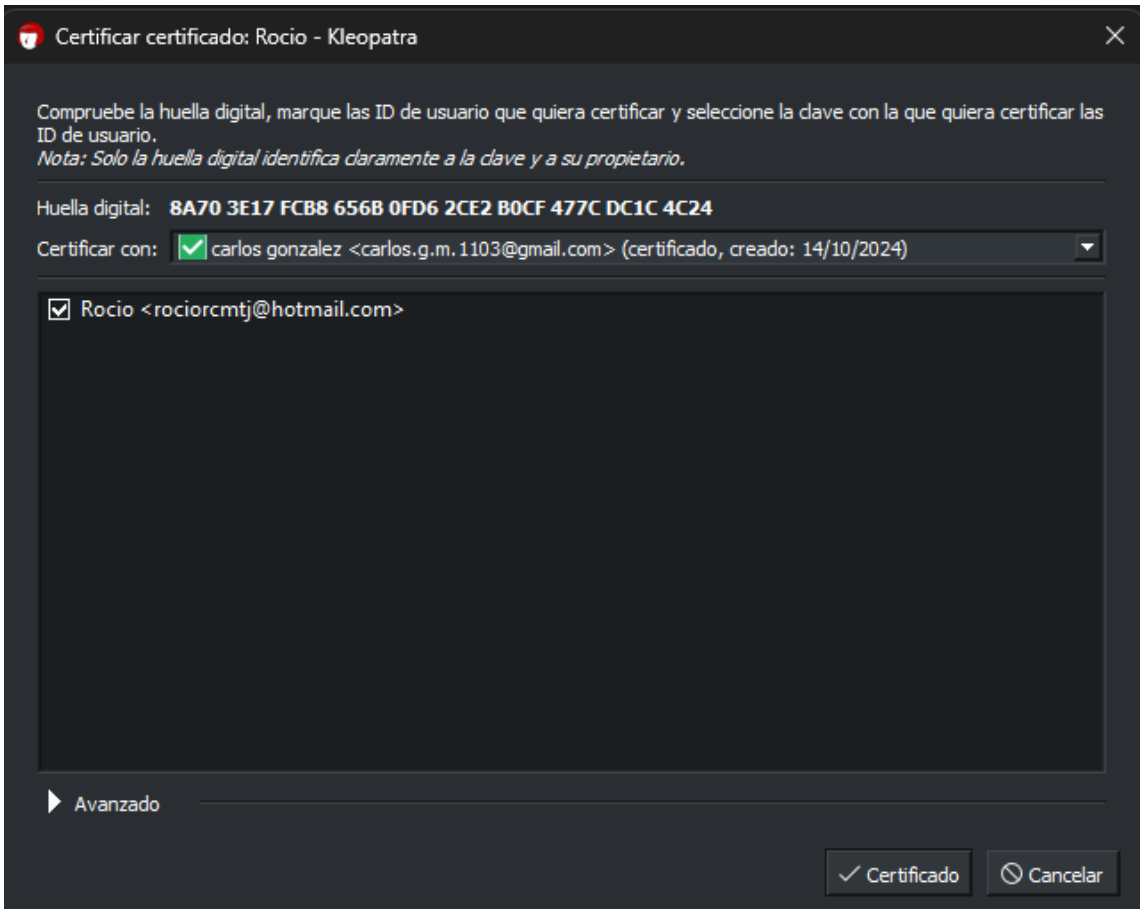
Una vez que le demos a exportar y lo guardaremos en el escritorio veremos el siguiente archivo.



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

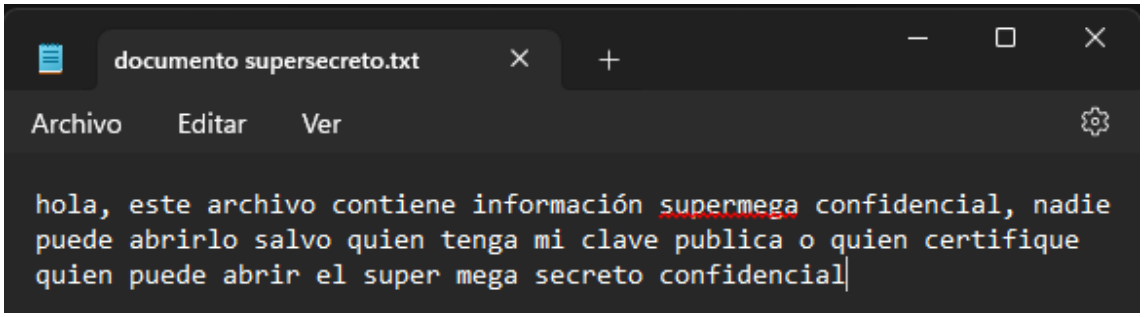


Una vez que le demos a importar certificados nos saldrá la siguiente ventana.

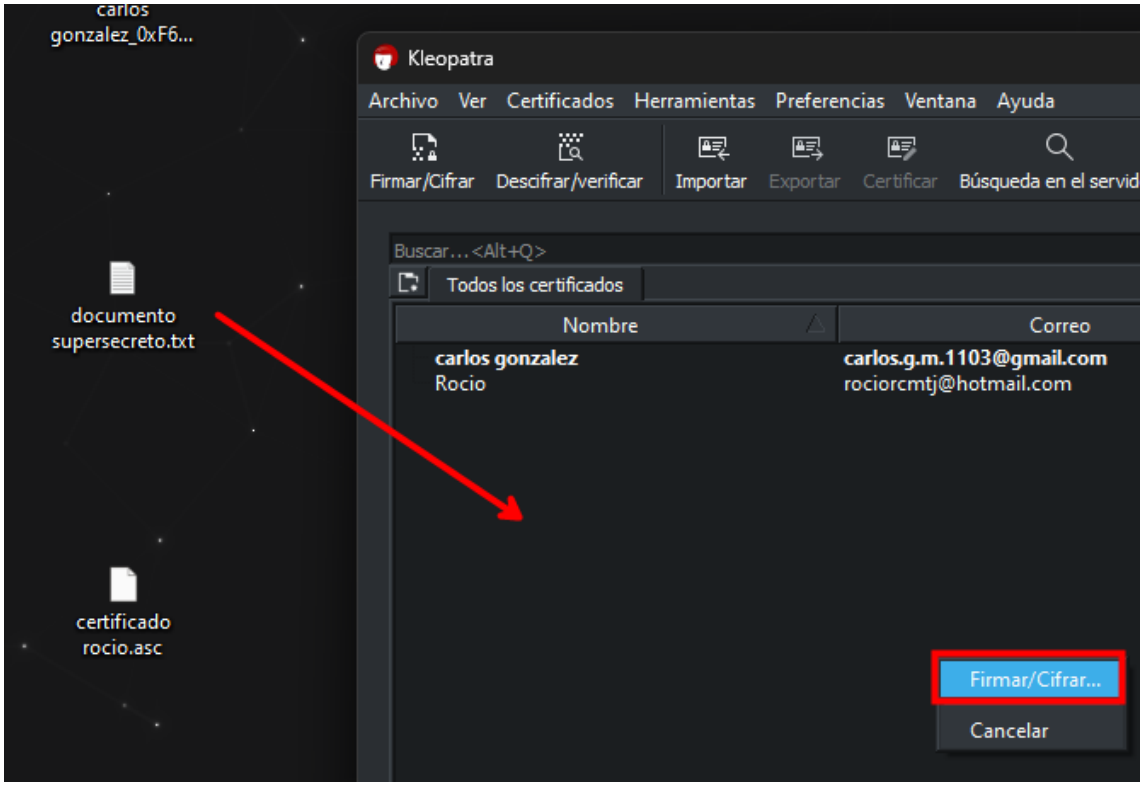


Y le daremos a “Certificado”.

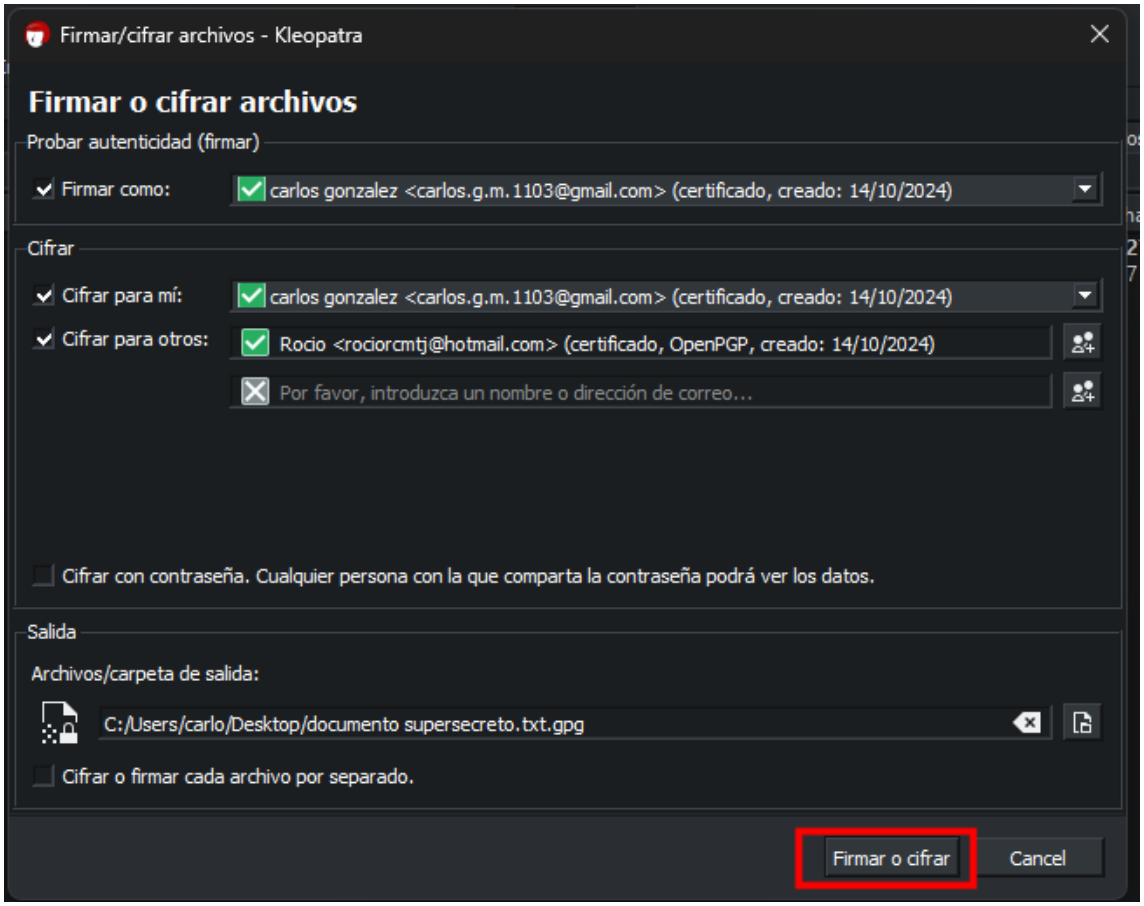
Una vez que tenemos los dos certificados procederemos ha hacer un archivo llamado “documento supersecreto.txt”.



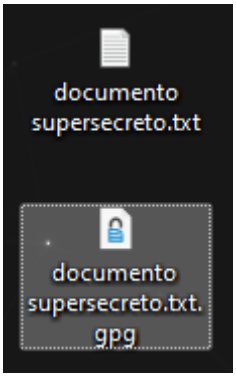
Una vez tenemos el documento guardado, lo que haremos será arrastrar el archivo a Kleopatra y le daremos a firmar/cifrar.



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



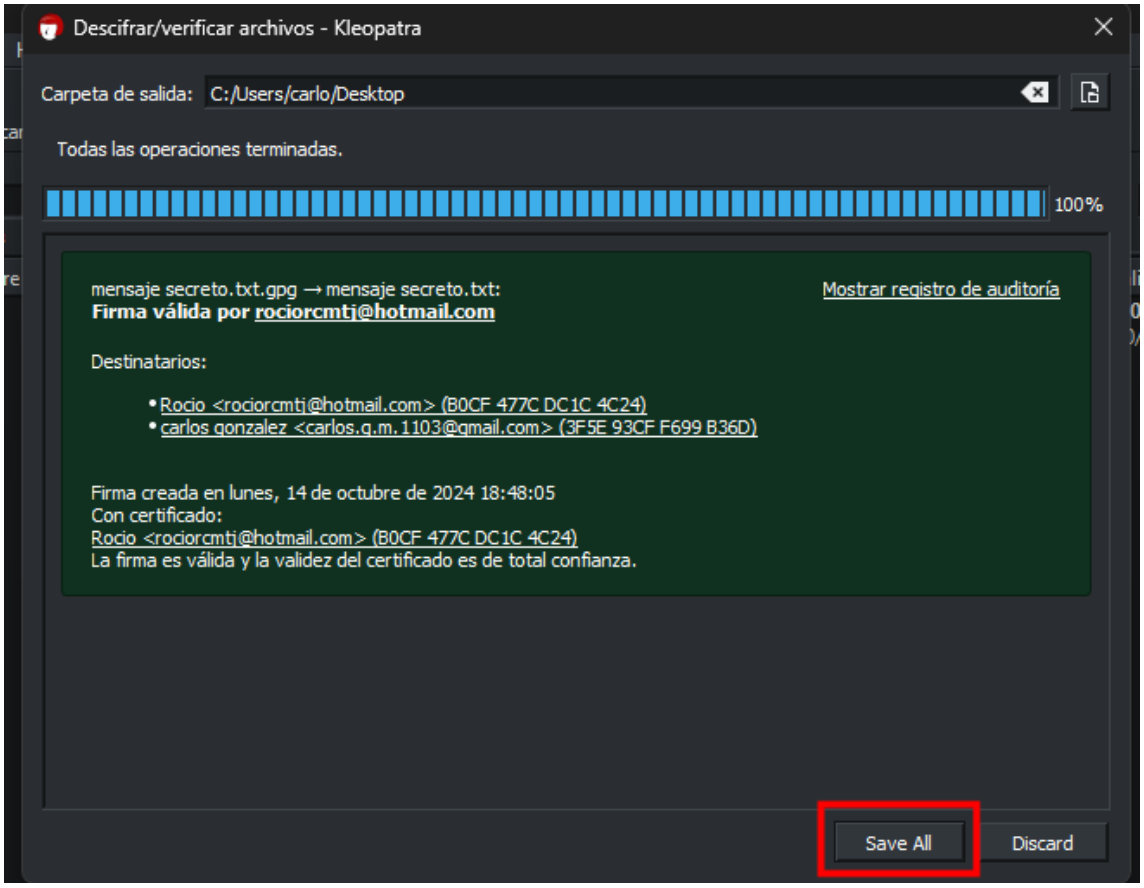
Le daremos a cifrar para otros y elegiremos el certificado que hemos importado anteriormente.



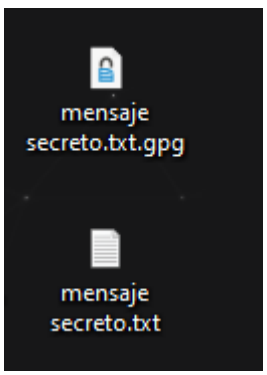
Una vez que le demos a firmar o cifrar nos saldrá el siguiente archivo.

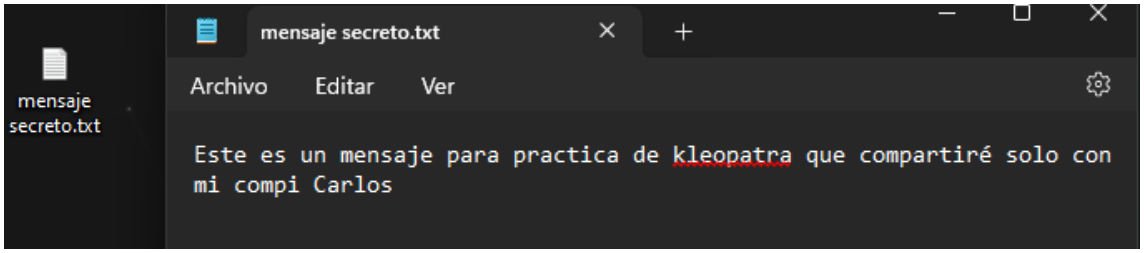
Ahora con otro documento que ha sido firmado con mi clave, podemos desencriptarlo.

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



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



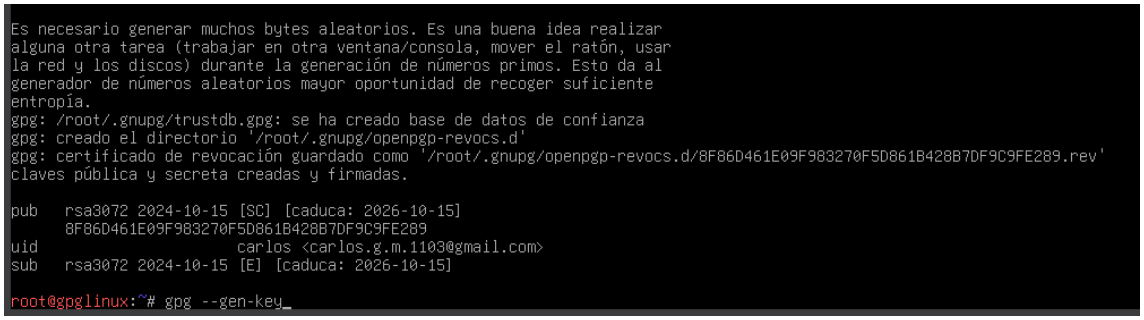


Y como podemos comprobar podemos visualizar el contenido del archivo.

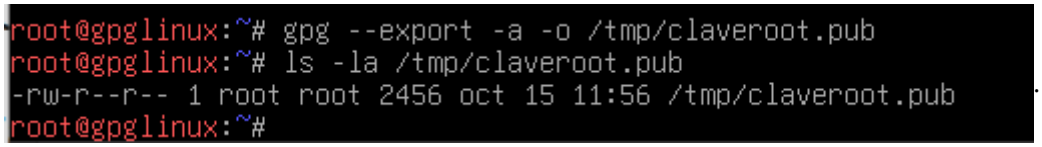
2. Linux

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”.

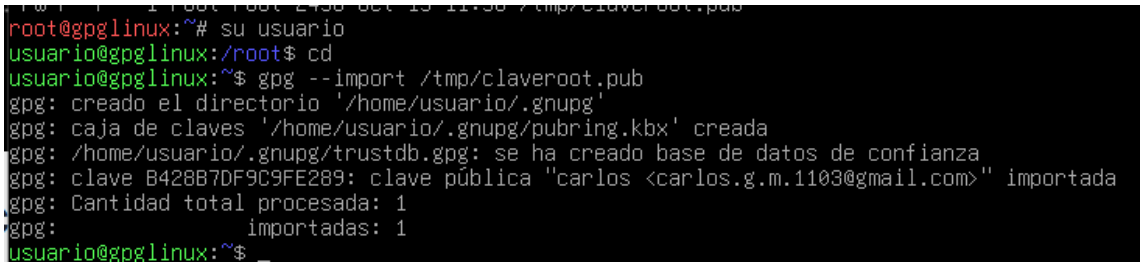
Una vez instalado el paquete procederemos a instalar con el comando “gpg –gen-key”.



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

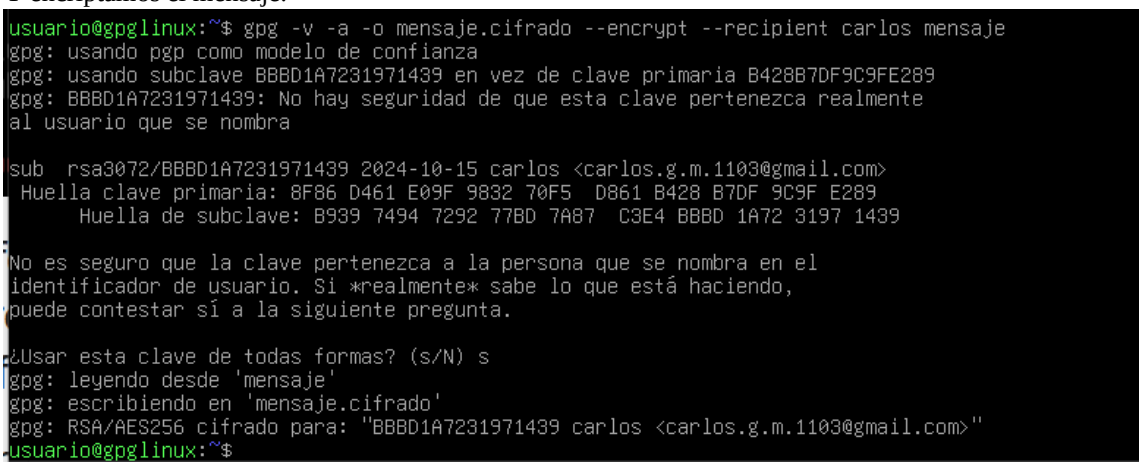


Una vez que estamos con “usuario” importaremos la clave.

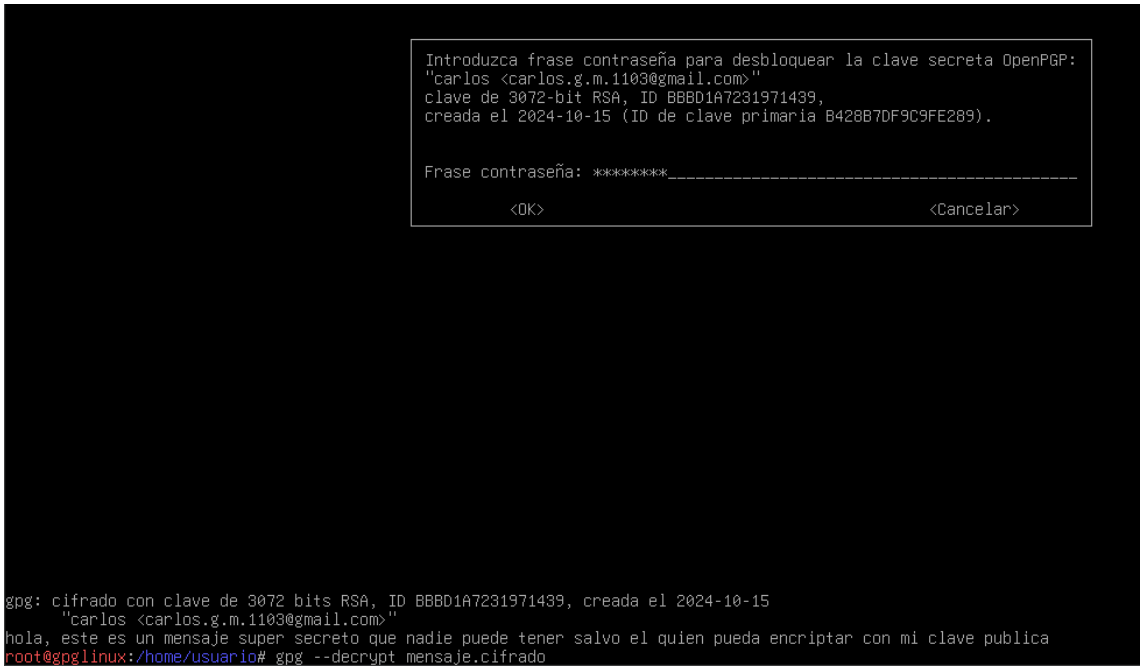


Ahora escribiremos un mensaje.

Y encriptamos el mensaje.



Una vez encriptado con el otro usuario lo desencriptaremos.



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.