Universidad Nacional Autónoma de México

SECRETARÍA DE DESARROLLO INSTITUCIONAL

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

GUÍA DE INSTALACIÓN, CONFIGURACIÓN Y USO DEL SOFTWARE KLEOPATRA PARA EL CIFRADO Y DESCIFRADO ASIMÉTRICO DE DIRECTORIOS Y ARCHIVOS

Manuel I. Quintero Martínez

Jesús Enrique Pacheco Franco

Coordinación de Seguridad de la Información. UNAM CERT

Ciudad Universitaria. CDMX 28 de mayo de 2021

Contenido

Resumen

Este documento muestra cómo instalar, configurar y utilizar la herramienta *Kleopatra* para cifrar y descifrar documentos y carpetas haciendo uso del cifrado asimétrico.

Objetivo

Servir como guía para la instalación, configuración y uso de la herramienta *Kleopatra*.

Desarrollo

A lo largo de jornada laboral se utiliza una gran cantidad de archivos y mensajes, parte de los cuales son o pueden ser de dominio público y ello no representa un peligro para la organización en caso que lleguen a manos de terceros. Sin embargo, cuando se trata de documentos confidenciales que pueden poner en riesgo a la organización, si se utilizan de manera inadecuada, o requieren un alto grado de confidencialidad -como el resguardo de datos personales-, surge la necesidad de proteger los documentos con un mecanismo que disminuya la posibilidad de que sean utilizados de formas no autorizadas.

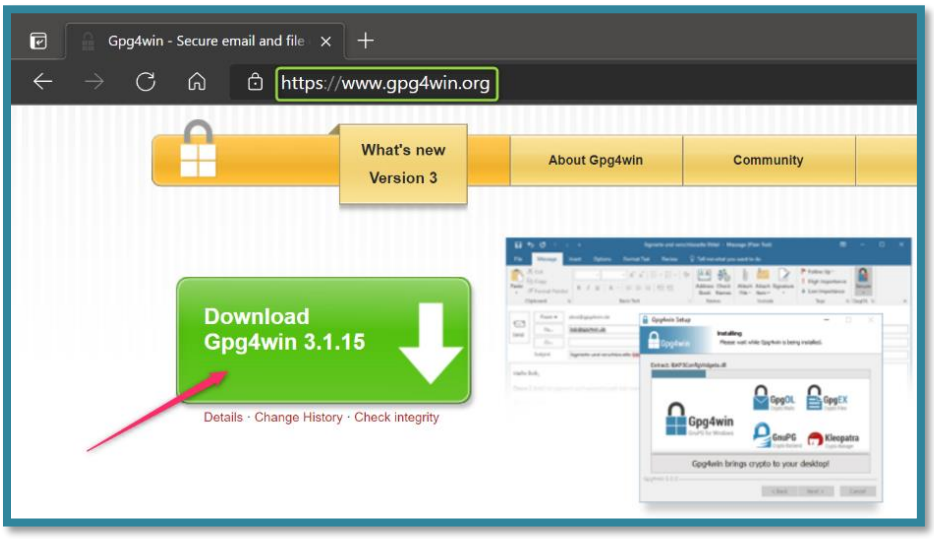
Una manera eficiente de preservar la confidencialidad de archivos y mensajes es a través del uso de la criptografía, cifrando los archivos para que estos se vuelvan accesibles solo si se cuenta con la llave específica para ello. Existen varios tipos de cifrado y cada uno tiene sus ventajas y desventajas e incluso hay tecnologías que implementan varios tipos de cifrado en conjunto. La herramienta *Kleopatra* hace uso de un tipo de cifrado asimétrico por medio de *GnuPG,* en el que la llave que se utiliza para cifrar no es la misma que se utiliza para descifrar.

En el cifrado asimétrico el usuario posee un par de llaves denominadas llave pública y llave privada. La llave pública puede ser compartida con cualquier otro usuario, ya que es la que se utiliza para el cifrado, el cual puede realizar cualquier persona, mientras que la llave privada, que el dueño no deberá compartir con nadie, es la que se requiere para descifrar la información.

Para ello, se puede hacer uso de GnuPG, una herramienta de línea de comandos que implementa un estándar que permite cifrar, descifrar y firmar datos y comunicaciones. También cuenta con funciones para una fácil integración con una gran cantidad de aplicaciones y bibliotecas *frontend* (parte de la aplicación que interactúa con el usuario). *Gpg4win* es la implementación oficial para Windows de *GnuPG* que es código abierto, y viene precargada con una interfaz de usuario llamada *Kleopatra*, que es un programa con interfaz gráfica que se utiliza para cifrar, descifrar y firmar archivos y carpetas de forma sencilla, además también cuenta con una funcionalidad de gestión de llaves.

Instalación y configuración de Gpg4win

A continuación, se describen los pasos a seguir para instalar y configurar la herramienta **GnuPG (GPG)** en un equipo Windows.



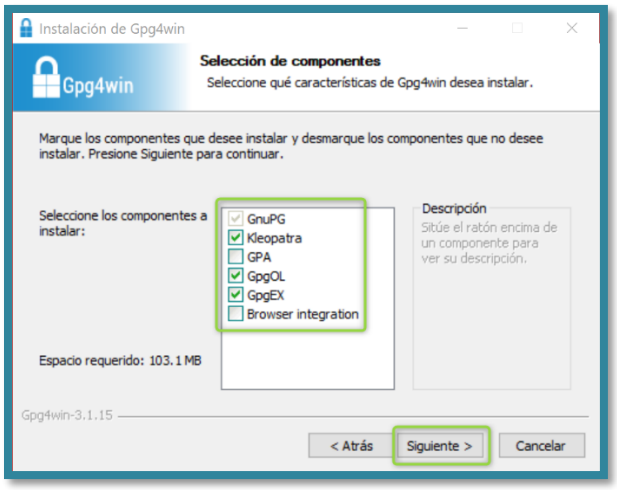
Descargar el software desde la siguiente página web dando clic en el botón "**Download**".
https://www.gpg4win.org/

Aparecerá la pregunta “si desea donar dinero para continuar con la mejora del proyecto **Gpg4win”**, se puede seleccionar la opción "**$0**" y dar clic en "**Download**".

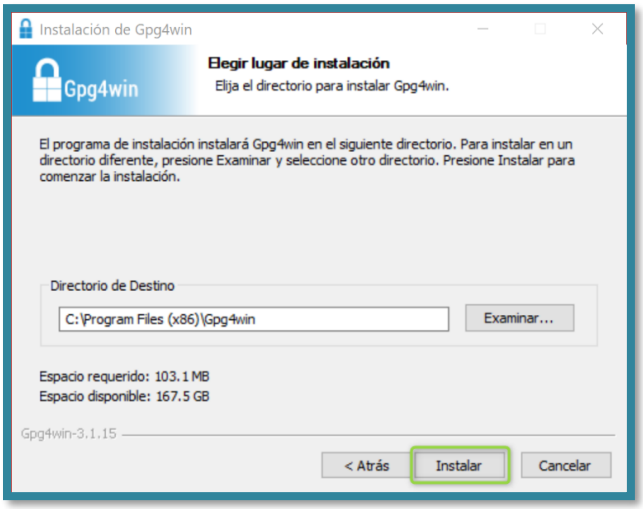
Una vez que se descarga el programa, dar doble clic sobre el ejecutable y se iniciará automáticamente el asistente de instalación. Aparecerá la pregunta “si desea realizar cambios en el equipo”. Dar clic en "**Yes/Sí**".

Seleccionar el idioma que se prefiera y dar clic en "**OK**". En esta guía se instalará el software seleccionando el idioma español.

Dar clic en "**Siguiente**".

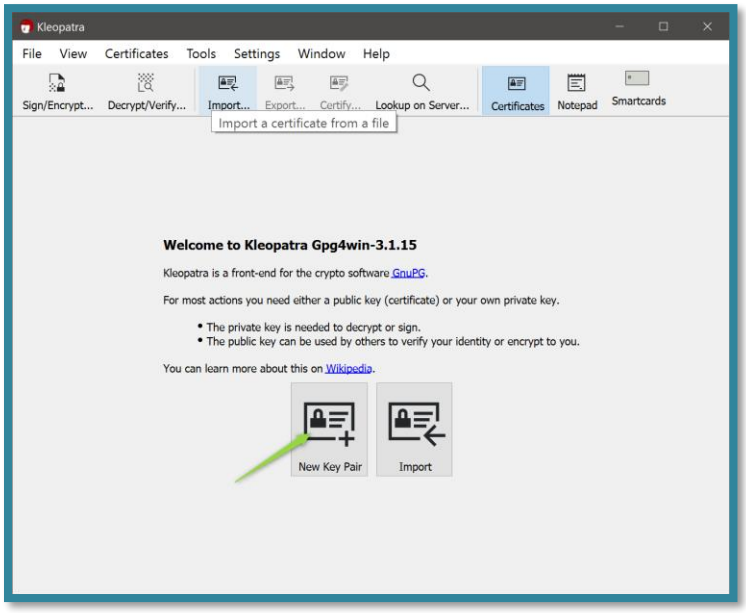


Marcar las opciones que se indican y dar clic en "**Siguiente**".

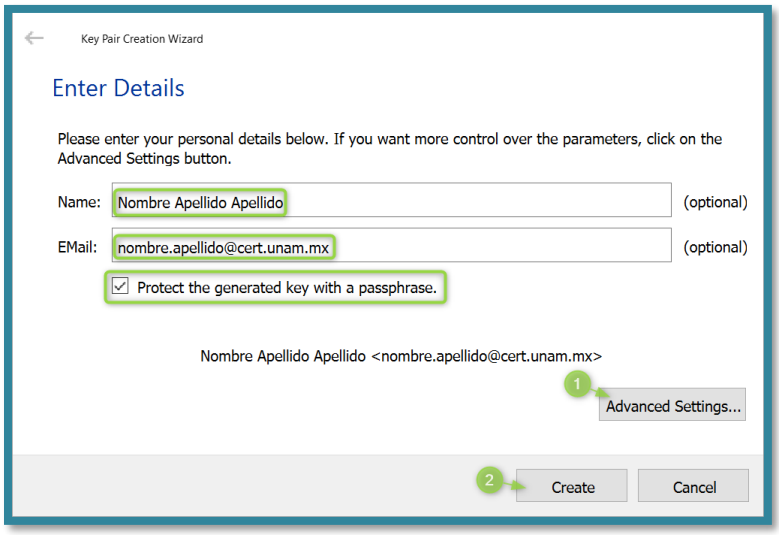


Generación de llaves

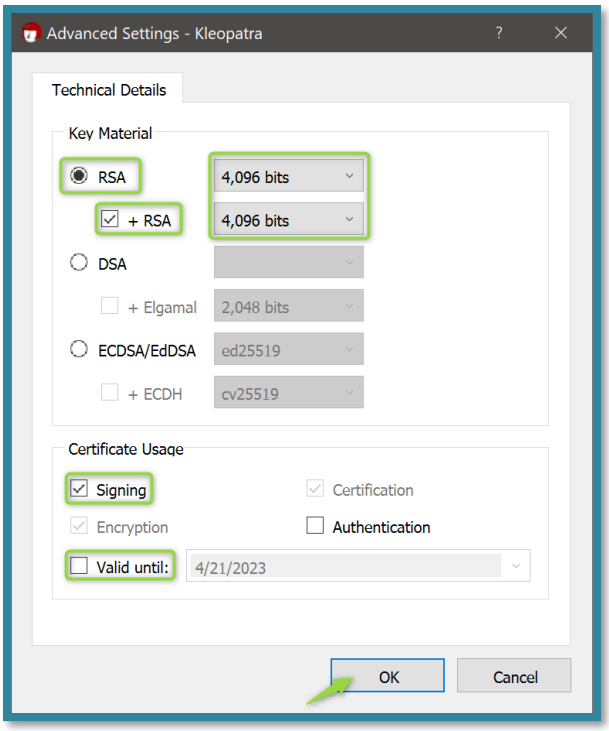
Las llaves son las que permitirán realizar el cifrado de la información. Es importante mencionar que la llave pública puede distribuirse a cualquier persona para que sea utilizada para cifrar de tal forma que sólo quien posee la llave privada correspondiente pueda descifrarlo. En ninguna circunstancia se debe compartir la llave privada porque podría permitir a personas no autorizadas descifrar información.



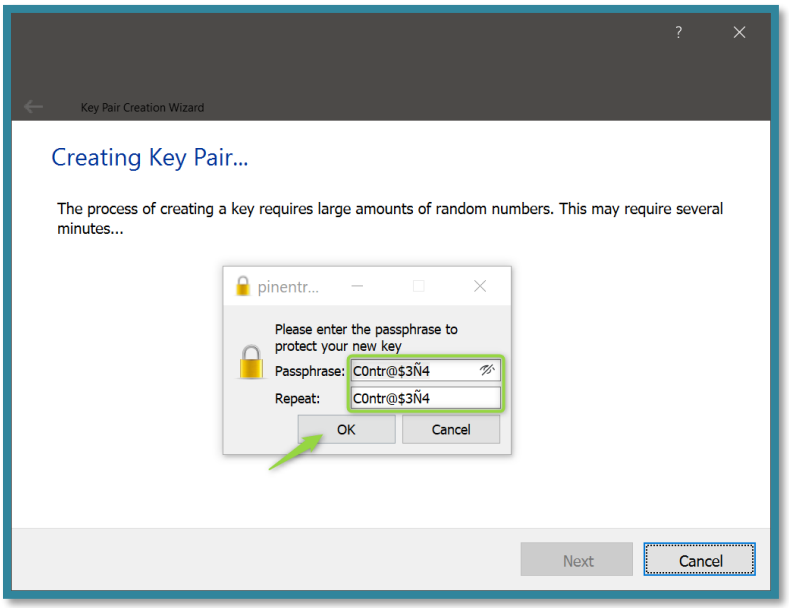
Abrir el programa *Kleopatra* y dar clic en la opción "**New Key Pair**".



Llenar los campos "**Name**", "**EMail**" con los datos correspondientes, marcar la casilla "**Protect the generated key with a passphrase**" para proteger la llave privada con una contraseña y posteriormente abrir las opciones avanzadas (**Advanced Settings…**) y así configurar las características de las llaves.



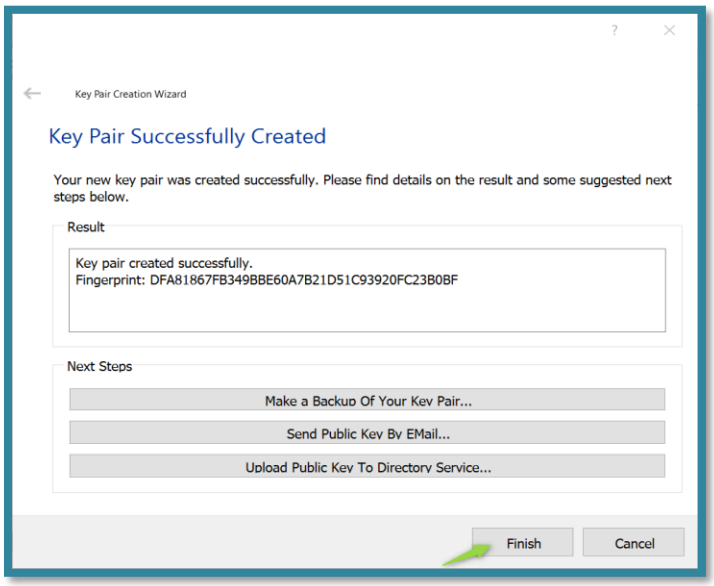
Configurar las opciones como en la imagen y dar clic en "**OK**".

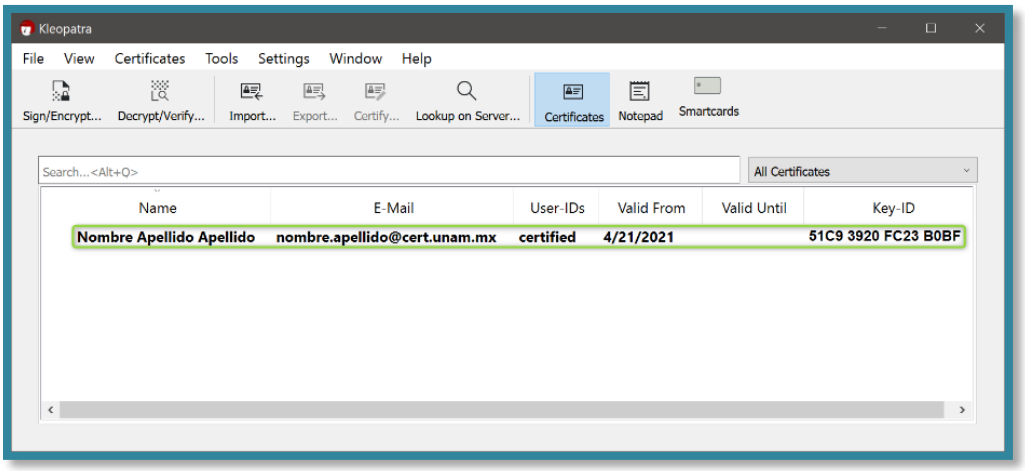


Proporcionar la contraseña de la llave privada dos veces y a continuación dar clic en "**OK**".

Proporcionar una contraseña que cumpla con las políticas de la organización y guardarla muy bien, ya que es la que se utilizará para firmar y descifrar los archivos y carpetas. Se recomienda que tenga 12 o más caracteres, incluyendo mayúsculas, minúsculas símbolos y números, y que sea fácil de recordar por quien la establece, pero difícil de obtener por otros.

Puede encontrar una guía para la generación de contraseñas seguras en el siguiente artículo: https://revista.seguridad.unam.mx/numero-15/password-fu-gu%C3%AD-f%C3%A1cil-para-contrase%C3%B1-realmente-seguras

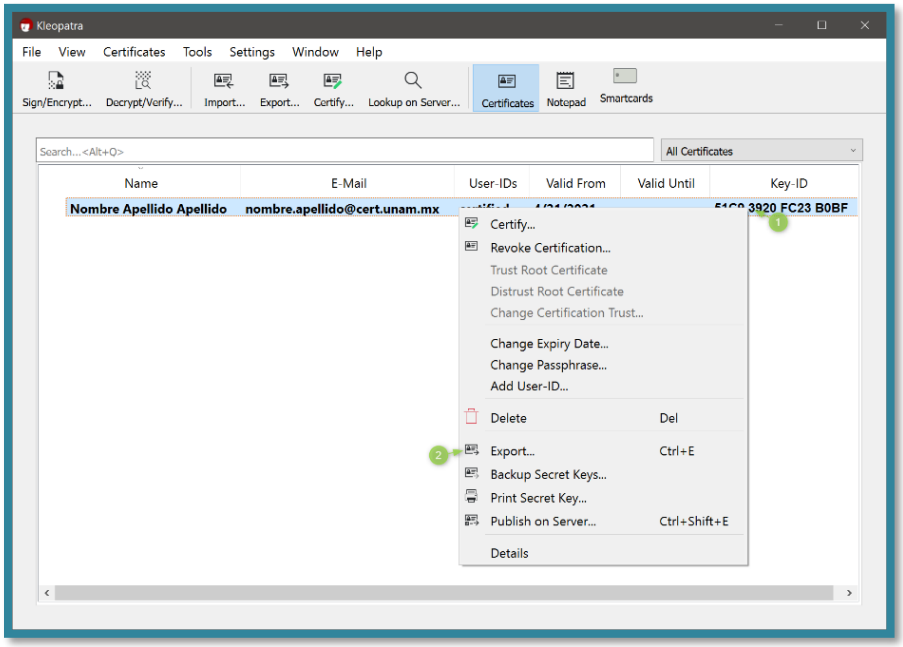




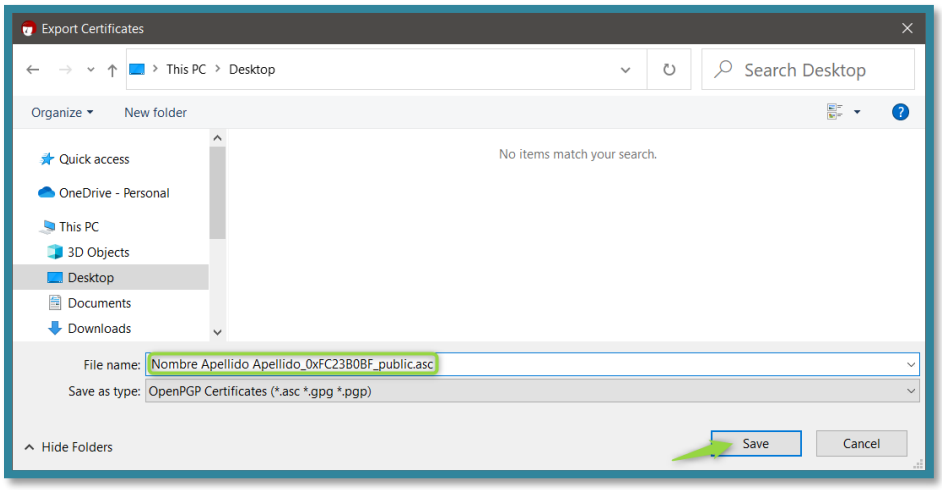
Exportar y compartir llaves

Llave pública

La llave pública es la que se utiliza para realizar el cifrado de datos, y puede ser compartida con cualquier usuario sin ningún riesgo ya que para enviar un mensaje cifrado a una persona primero se deberá contar su llave pública; una vez que se tiene, es posible utilizarla para cifrar los datos y la persona será capaz de descifrarlos con su llave privada.



Para exportar la llave pública propia se tiene que acceder a *Kleopatra*, dar clic derecho en la llave que se desea exportar y a continuación seleccionar la opción "**Export…**"



Seleccionar la carpeta donde se desea almacenar la llave y finalmente dar clic en "**Save/Guardar**".

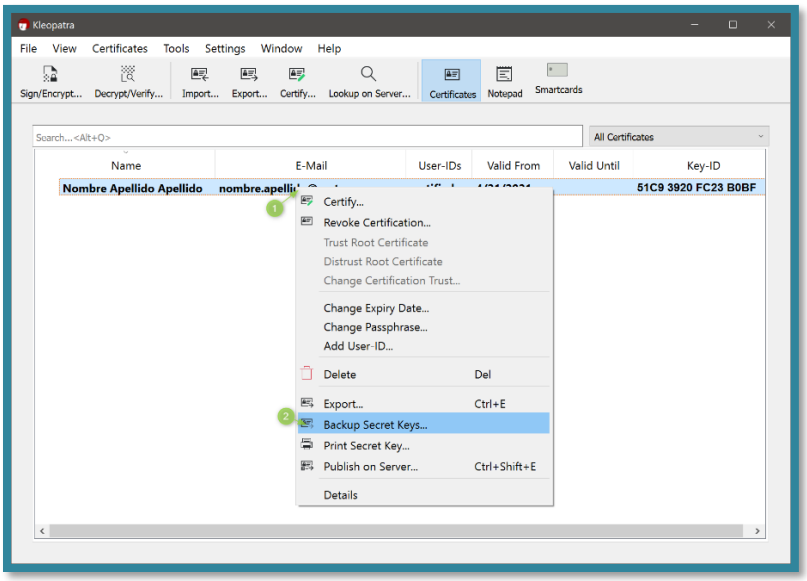
El archivo que se genera es la llave pública y puede ser compartido con otros usuarios vía correo electrónico o en un servidor de llaves. Una vez que se tiene una llave pública es posible enviar datos cifrados al dueño de esta. Es importante que cuando la reciba el destinatario, se verifique la autenticidad de la llave enviada.

Llave privada

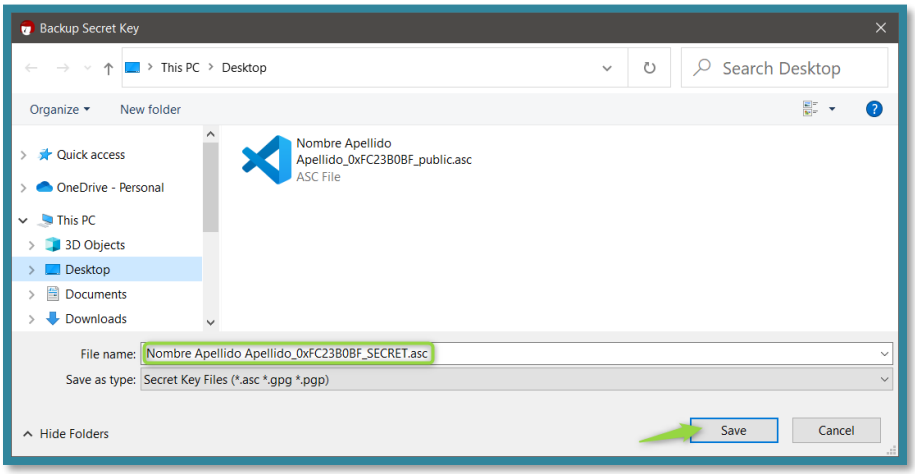
La llave privada es la que se utiliza para descifrar, y dado que está protegida por una contraseña, no es posible descifrar datos sin ella. Es por lo que se recomienda no compartirla bajo ningún motivo. Si se requiere que diversos usuarios descifren un archivo, entonces cada uno deberá generar un par de llaves, y compartir la pública con la persona que cifrará la información, pues es factible que el mismo archivo sea cifrado con diversas llaves públicas, de forma que cualquiera de ellos pueda extraer la información.

Generalmente esta llave permanece dentro de *Kleopatra* porque no se debe de compartir con nadie más, pero es posible exportarla por si se desea respaldar o si se desea usar en alguna otra aplicación.

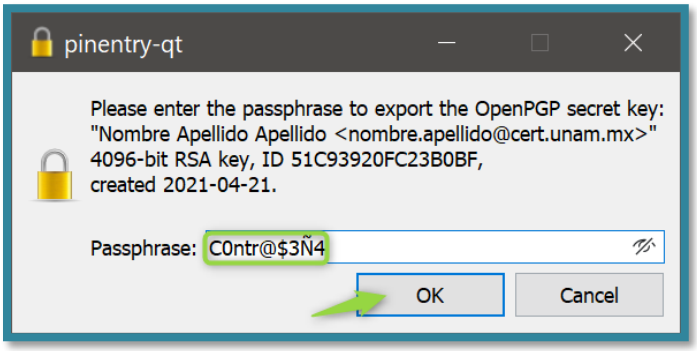
Para exportar la llave se sigue un proceso bastante similar al de la exportación de la llave pública, sin embargo; en este caso se preguntará por la contraseña que protege a la llave privada para poder exportarla.



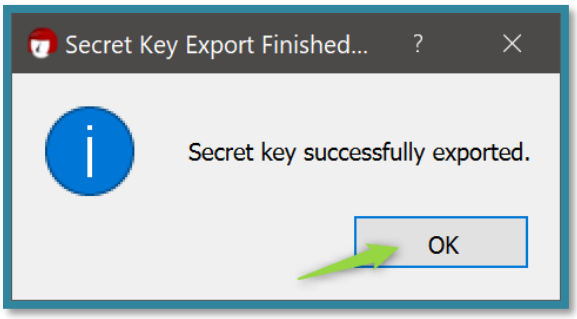
Clic derecho y seleccionar la opción "**Backup Secret Keys…**"



Seleccionar la carpeta donde se desea almacenar la llave y finalmente dar clic en "**Save/Guardar**".



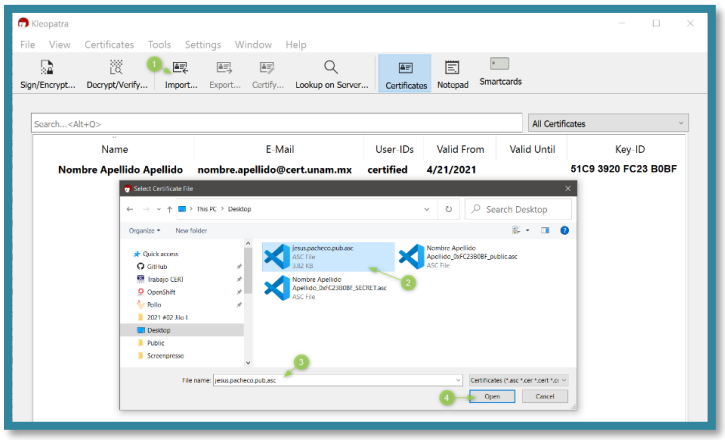
Proporcionar la contraseña de la llave privada y dar clic en "**OK**".



Dar clic en "**OK**".

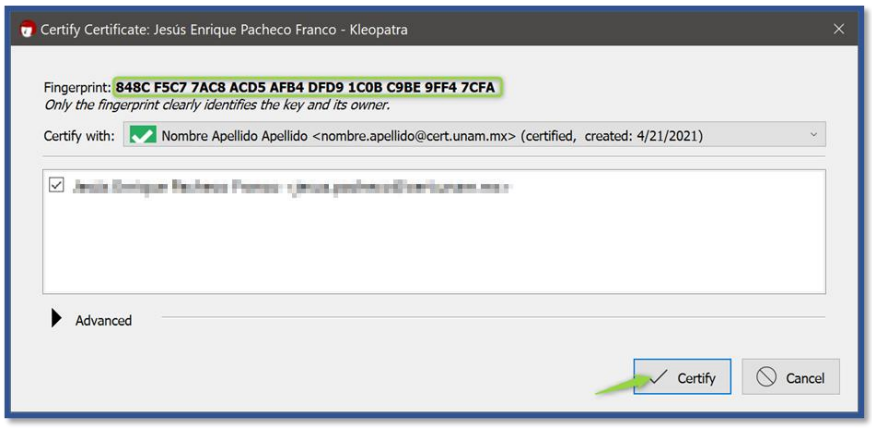
Importar llave pública

Una vez que se recibe la llave pública de otros usuarios, estas se pueden importar para poder cifrar datos con ellas utilizando Kleopatra. El proceso de importación de llaves se describe a continuación:

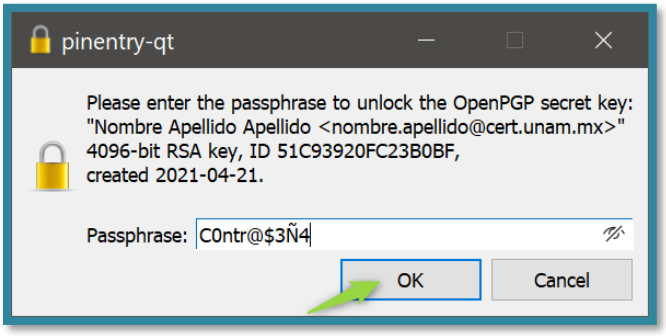


Seleccionar la opción "**Import…**", seleccionar la llave que se desea importar en el sistema de archivos y finalmente dar clic en "**Open/Abrir**".

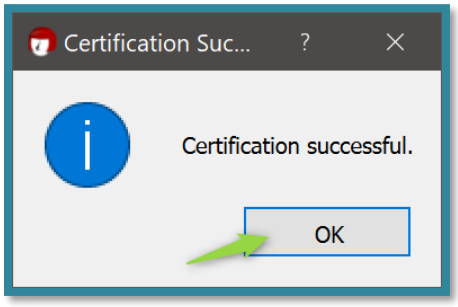
Se advierte que antes de importar la llave se debe de verificar el "**Fingerprint**" de la llave con el dueño.



El "*fingerprint*" es un conjunto de caracteres único que identifican a una llave para validarla. Se debe preguntar al dueño de la llave cual es el "**Fingerprint**" y compararlo con el que está mostrando Kleopatra, si ambos son iguales entonces la llave es correcta y se debe dar clic en "**Certify**".



Se proporciona la contraseña de la llave privada que se usó para certificar la nueva llave pública. En este caso **<nombre.apellido@cert.unam.mx>**.

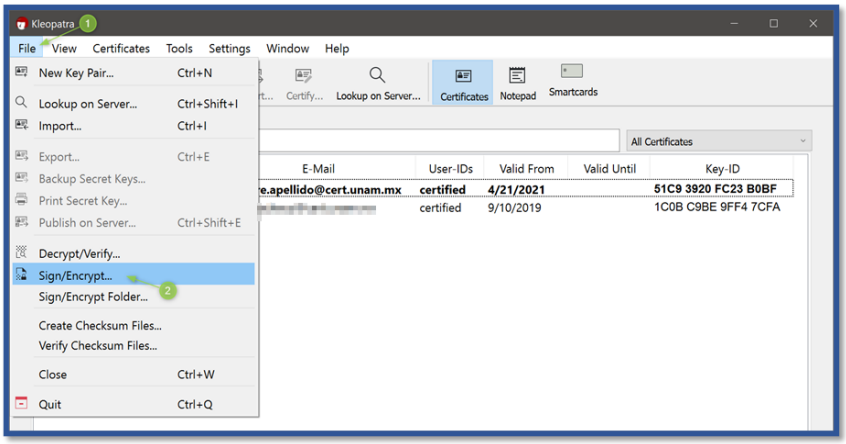


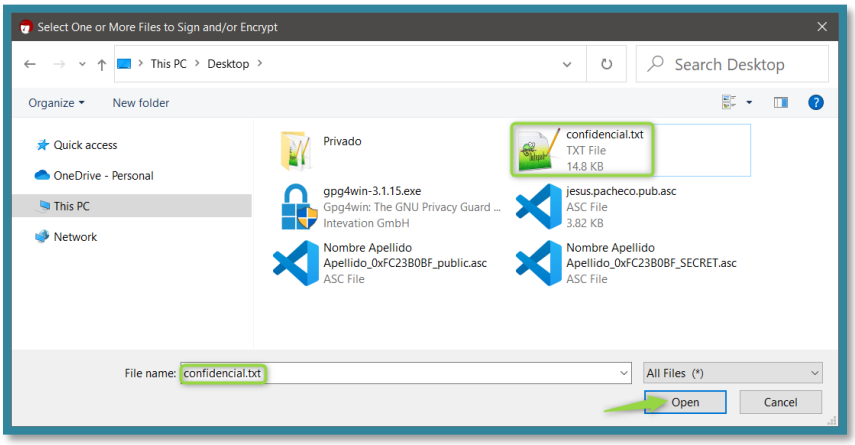
Finalmente dar clic en "**OK**".

Cifrado de archivos y carpetas

Cifrado de archivos

Para cifrar un archivo se tiene que seleccionar la pestaña "*File*" y a continuación seleccionar la opción "**Sign/Encrypt…**".

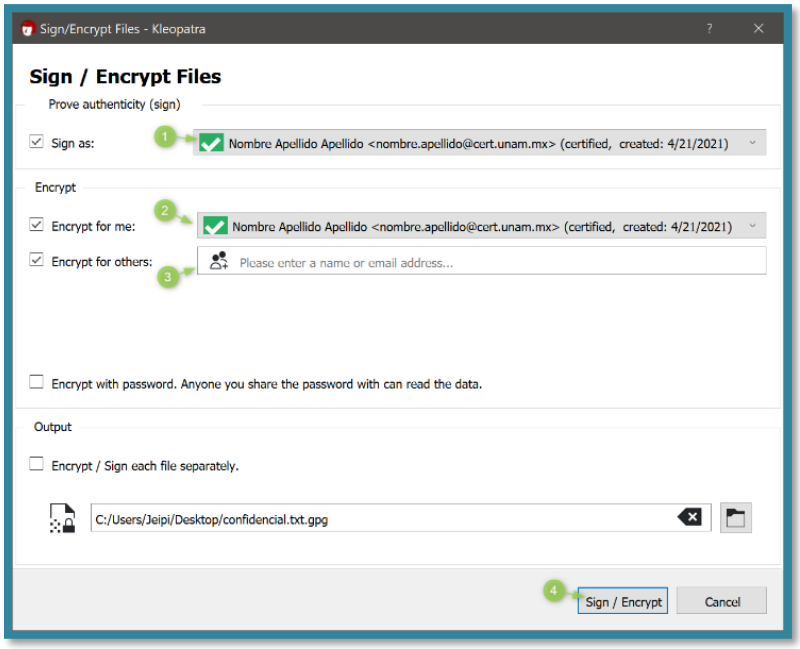


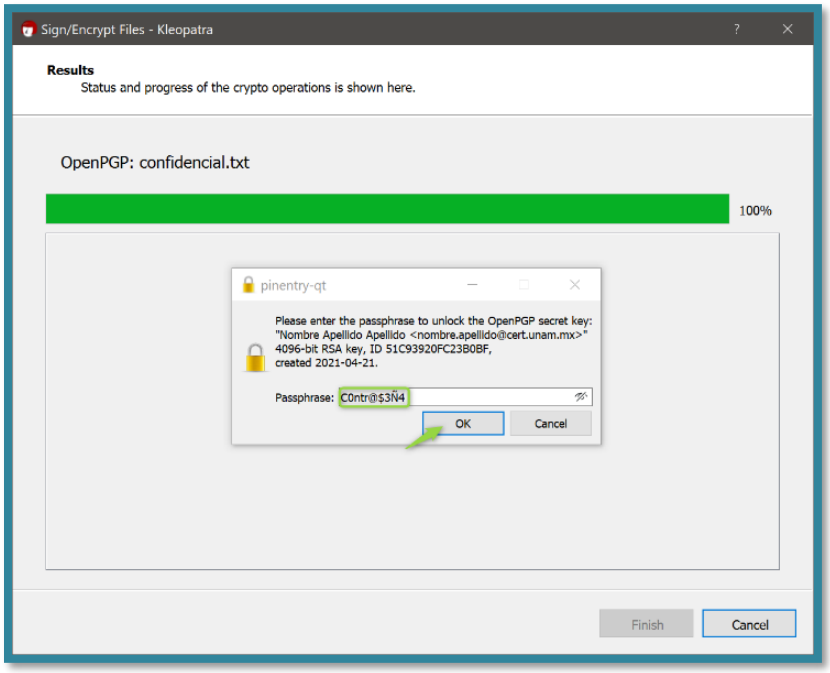


Seleccionar el archivo que se desea cifrar y dar clic en "**Open/Abrir**".

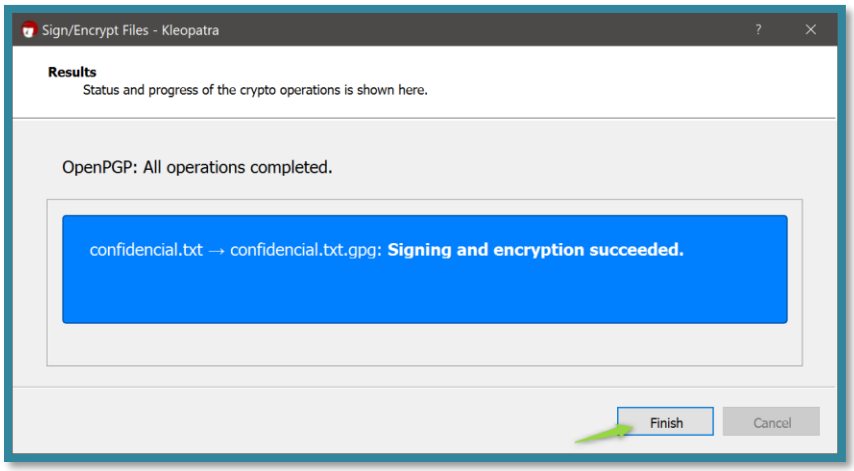
Indicar si se desea firmar el archivo a cifrar o no (**Sign as**). Firmar el archivo permite a quien lo descifra conocer la identidad de quien lo cifró, esta opción puede habilitarse o no según se desee. Posteriormente, para cifrar, se selecciona el destinatario del documento. Si se selecciona la opción de cifrarlo para uno mismo (**Encrypt for me**) se cifrará el archivo y se podrá descifrar por que se cuenta con la llave privada. Si se selecciona cifrar para otros (**Encrypt for others**) una vez que se cifre el archivo, este ya no podrá ser descifrado, ya que se cuenta con la llave pública de otros, pero no con su llave privada.

En este paso puede seleccionar a todos los usuarios que podrán descifrar el archivo o carpeta, por lo que es necesario contar de antemano con sus llaves públicas. Una vez que se configuran las opciones dar clic en "**Sign/Encrypt**".

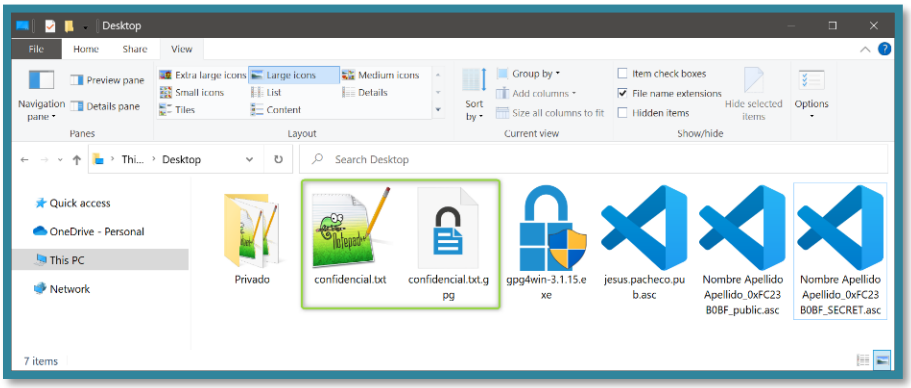




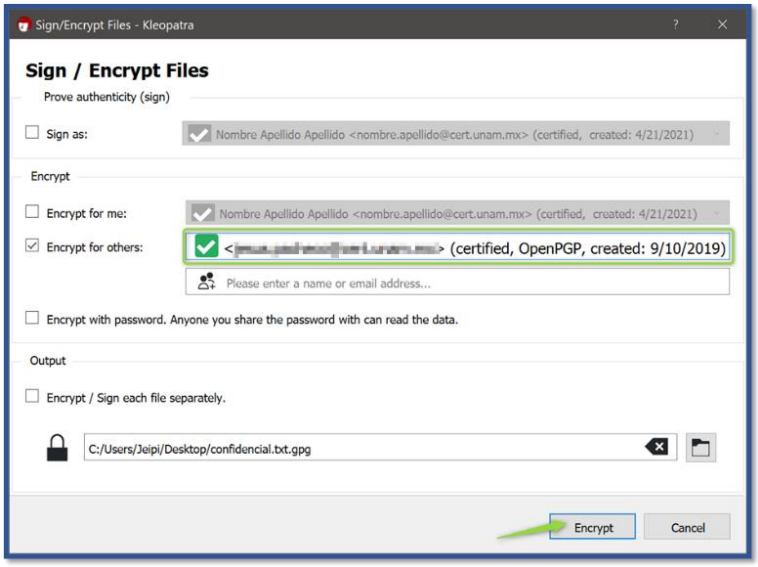
Si se selecciona cifrar para uno mismo (**Encrypt for me**) se tiene que ingresar la contraseña de la llave privada y a continuación dar clic en OK.



Finalmente se da clic en "**Finish** "y el archivo quedará cifrado.

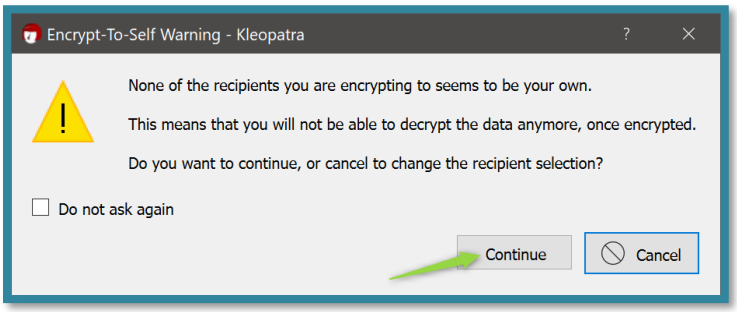


Como se observa se generó un nuevo archivo con la extensión "**.gpg**", este es el archivo cifrado, y también se mantuvo el archivo original. Si solo desea conservar el archivo cifrado se puede borrar el original con una herramienta de borrado seguro.

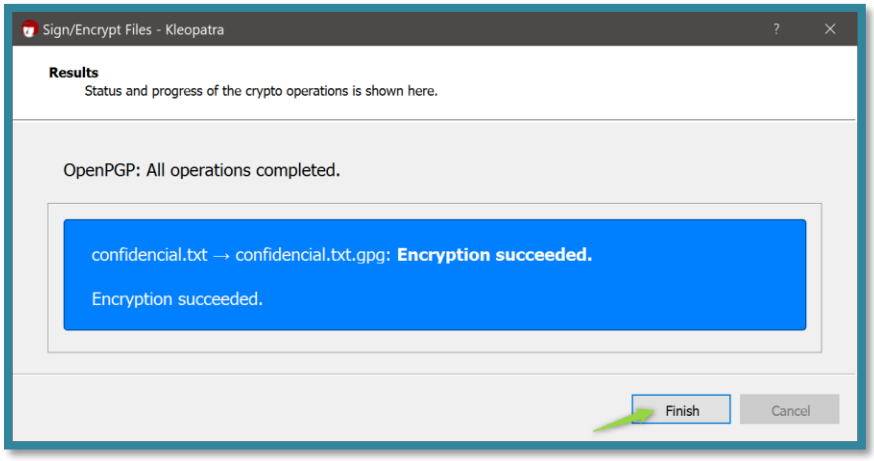


En este otro ejemplo de cifrado de archivo para otra persona, se está haciendo uso de la llave pública de un usuario para cifrar el archivo y no se está firmando, es decir que no habrá manera de validar quién fue el responsable del cifrado del archivo.

Al dar clic en *Encrypt* se muestra una ventana advirtiendo que no se cuenta con la llave privada del o los usuarios, entonces no será posible descifrar el archivo y solo él podrá descifrarlo.



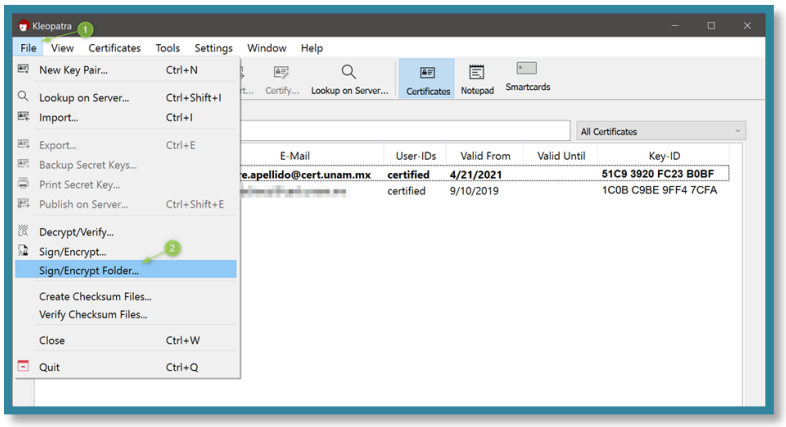
Dado que es un archivo que se va a enviar a otra persona, no hay mayor problema, ya que la otra persona podrá descifrar lo que se le envíe.



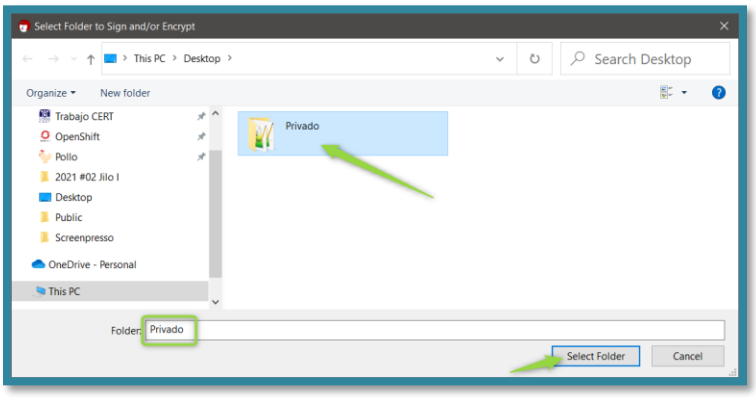
El cifrado se realizó correctamente, dar clic en "**Finish**" para terminar.

Cifrado de carpetas

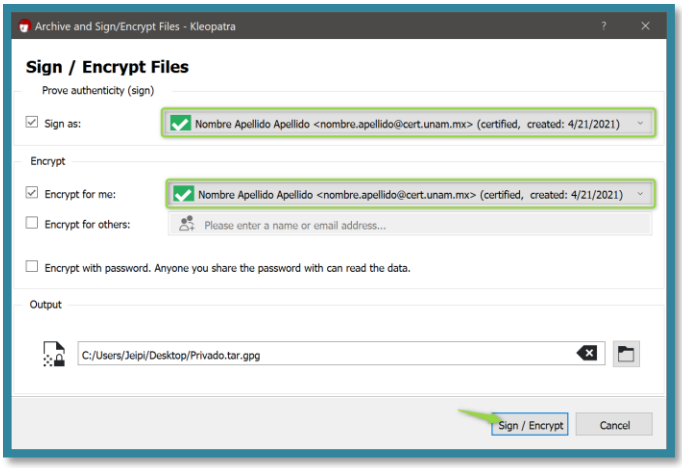
El proceso para cifrar una carpeta es exactamente el mismo que el del cifrado de un archivo, lo único que cambia es que, en lugar que se va a cifrar un archivo, se indica que se desea cifrar una carpeta.



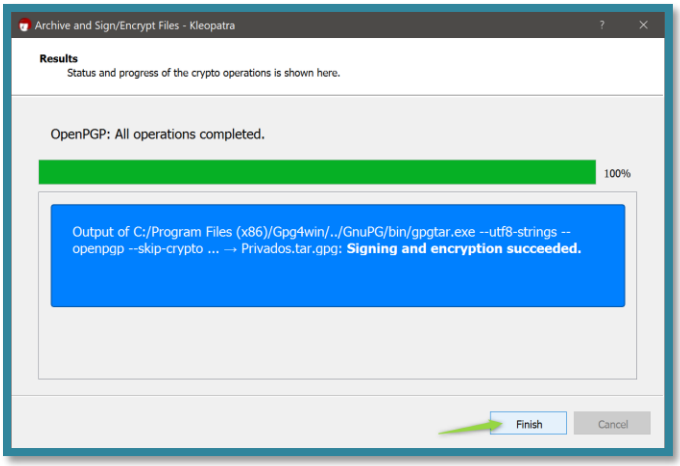
Una vez se selecciona "**Sign/Encrypt Folder…**" seleccionar la carpeta a cifrar y dar clic en "**Select Folder**".



Indicar si se desea firmar, cifrar para uno mismo o para otros y dar clic en "**Sign/Encrypt**".

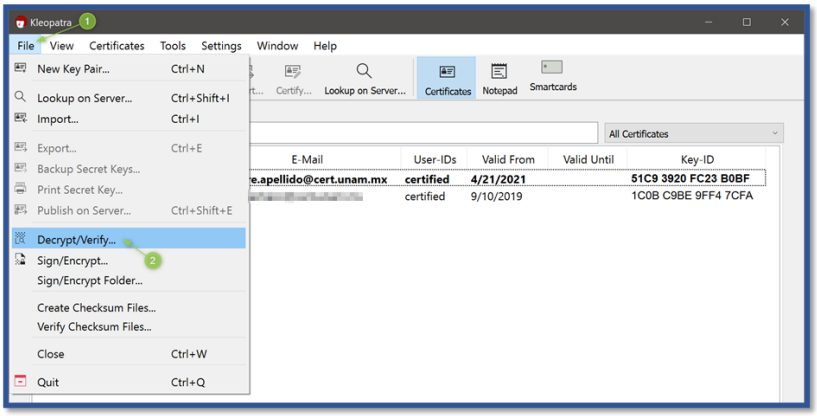


Proporcionar la contraseña de la llave privada si es que se pide y finalmente dar clic en "**Finish**" para terminar.

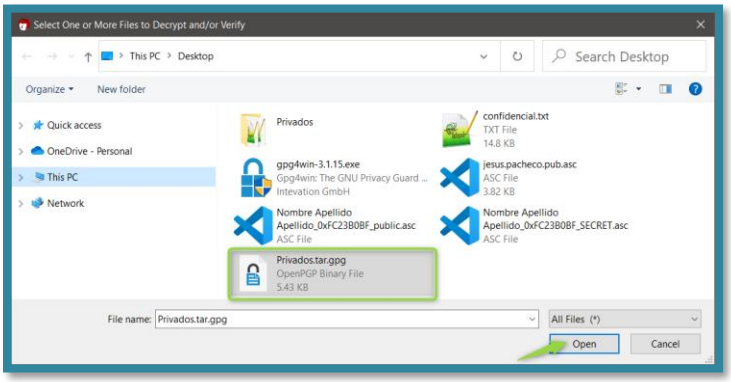


Descifrado de archivos y carpetas

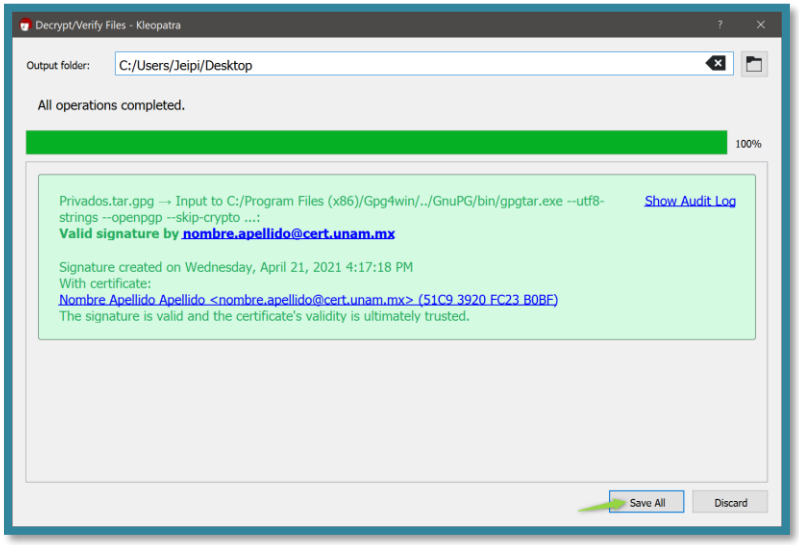
El proceso para descifrar archivos y carpetas es exactamente el mismo, pues ambos archivos tienen la extensión "**.gpg**". Para descifrar un archivo o carpeta dar clic en la pestaña File, opción "**Decrypt/Verify…**".



Seleccionar el archivo/carpeta a descifrar y dar clic en "**Open/Abrir**".



Finalmente dar clic en "**Save All**" para guardar el archivo/carpeta descifrada.



El archivo/carpeta se descifra dentro del mismo directorio donde se encuentra el archivo cifrado con extensión "**.gpg**".

Nota: Es posible que en algunas ocasiones se solicite la contraseña de la llave privada y en otras no, ya que esta se mantiene en memoria durante un cierto tiempo en la memoria cache dentro de *Kleopatra*, para hacer más rápido el proceso.

Referencias

- GnuPG

  https://gnupg.org/

Control de versiones

Versión	Fecha	Cambios	Realizado por
1.0	27 mayo 2021	Creación de documento	Pacheco Franco Jesús Enrique (UNAM-CERT) Quintero Martínez Manuel I. (UNAM-CERT)
1.0	28 mayo 2021	Correcciones de estilo	Villa George Laura (DGTIC-DSSI-DVRV) Luna González Lizbeth (DGTIC-DSSI-AAD) Romo Zamudio Fabián (DGTIC – DSSI)