ANEXO 9 – PROTOCOLO TÉCNICO PARA LA PRESENTACIÓN DE LAS OFERTAS ECONÓMICAS

A. ENVÍO DE DOCUMENTOS QUE CONFORMAN LAS OFERTAS ECONOMICAS

1. Para efectos del envío de las ofertas económicas, estas deberán ser remitidas a través de los correos electrónicos **ofertasaerocafe1@gmail.com** **ó** **ofertasaerocafe1a@gmail.com**, hasta el día y hora de cierre del proceso para que puedan ser abiertas durante la audiencia de apertura de la carpeta digital No.2.

2. Se adjunta a este documento el archivo ***Clave primaria PAUG-CA-01-2021*** que contiene la llave primaria generada por parte de la Unidad de Gestión del Patrimonio Autónomo AEROCAFE, con la cual el oferente deberá encriptar su oferta económica, utilizando la herramienta **Gpg4win**, también conocida como **Kleopatra**.

Clave primaria
PAUG-CA-01-2021.as

3. Seguido a esto el oferente deberá crear su clave privada con el aplicativo Kleopatra, siguiendo las instrucciones del manual de uso adjunto a esta comunicación. En caso de tener inquietudes enviar correo a **observacionesaerocafe1@gmail.com**, de conformidad a los plazos establecidos en el cronograma.

   Nota: ***Se recomienda realizar pruebas de encriptación de archivos antes de la fecha prevista para presentación de observaciones, con el propósito de resolver oportunamente cualquier inconveniente, duda o inquietud al respecto.***

4. Una vez recibidas todas las ofertas económicas, estas serán descargadas, guardadas y custodiadas en un disco duro externo por parte de la Unidad de Gestión del Patrimonio Autónomo AEROCAFE, hasta la fecha y hora de apertura de las propuestas económicas de los oferentes habilitados.

5. El día y hora previstos para la audiencia de adjudicación se dará apertura a las ofertas económicas, para lo cual cada uno de los oferentes habilitados deberá informar, de acuerdo al orden establecido por quien dirige la audiencia, la clave secundaria asignada en la herramienta Kleopatra para realizar la apertura inmediata de su oferta.

NOTA:

Se debe tener en cuenta que la capacidad de enviar archivos a través de correo electrónico es de 25 MB, en caso de que los documentos superen este tamaño, se recomienda utilizar la herramienta https://wetransfer.com/ la cual permite enviar archivos de hasta 2 GB.

Manuales

- ***Manual de instalación Kleopatra***

manual de instalación de Gpg4

- ***Manual de uso Kleopatra***

manual de uso de Gpg4win_kleopatra

B. ACCESO VIRTUAL A LA DILIGENCIA

1. El acceso virtual a la diligencia se hará por parte de los intervinientes a través del vínculo que será publicado mediante aviso en la página web de la Fiduciaria Colpatria (https://www.scotiabankcolpatria.com/fiduciaria/publica/productos/patrimonio-autonomo-aerocafe) y el SECOP 1 (https://www.contratos.gov.co/consultas/inicioConsulta.do).

2. El oferente deberá conocer y cumplir con los requerimientos técnicos, definidos en el literal C de este documento, como prerrequisito para acceder a la diligencia.

3. Podrán acceder virtualmente a la diligencia el personal designado de la Unidad de Gestión del Patrimonio Autónomo AEROCAFE, las partes, los apoderados y los oferentes.

Los canales virtuales estarán habilitados 15 minutos antes del inicio de la diligencia o actuación, con el propósito de que los intervinientes o interesados accedan a la plataforma y reporten al personal de Soporte Técnico de la Unidad de Gestión del Patrimonio Autónomo AEROCAFE, los inconvenientes que presenten, a afectos de superarlos antes del inicio de la diligencia.

C. REQUERIMIENTOS TÉCNICOS

1. Aplicaciones:

Las diligencias se llevarán a cabo haciendo uso de la aplicación tecnológica definida por la Unidad de Gestión del Patrimonio Autónomo AEROCAFE, la cual será debidamente informada mediante aviso.

2. Equipo de cómputo, tabletas y móviles:

Las aplicaciones tecnológicas se podrán descargar e instalar en dispositivos computadores con windows 10 en adelante y con mac OS X 10.11 en adelante, así como en dispositivos móviles android e iOS.

3. Vínculo de descarga de la aplicación:

La ruta de acceso al vínculo de descarga para la diligencia se comunicará mediante aviso en la página web de la Fiduciaria Colpatria (https://www.scotiabankcolpatria.com/fiduciaria/publica/productos/patrimonio-autonomo-aerocafe) y el SECOP 1 (https://www.contratos.gov.co/consultas/inicioConsulta.do).

4. Micrófono y cámara:

El equipo de cómputo, tableta o móvil utilizado deberá contar con dispositivos de audio y video que permitan visualizar la diligencia e intervenir en la misma, a fin de garantizar la participación de todos los interesados.

5. Capacidad de acceso a internet:

Para participar en la diligencia, los intervinientes deben contar con una conexión de internet con ancho de banda de mínimo 5 megas.

ANEXO 2

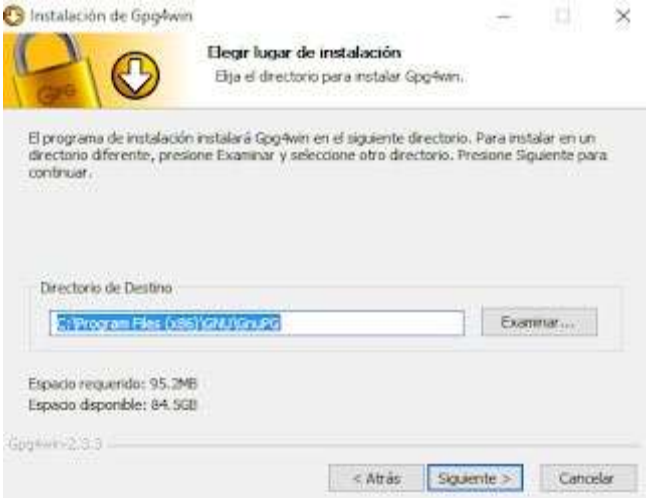
MANUAL DE INSTALACIÓN

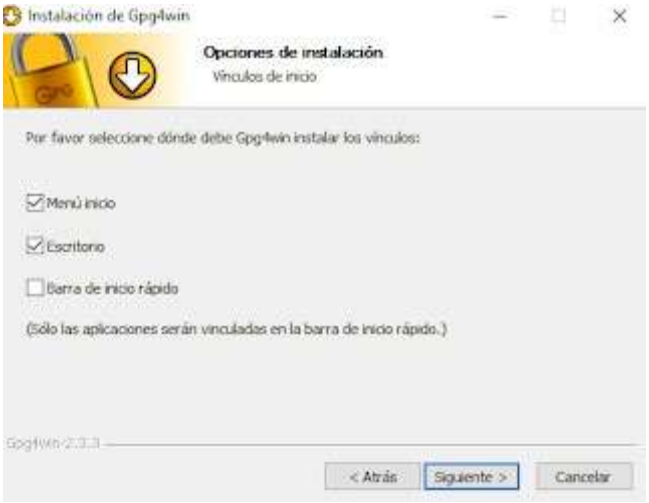
1. Instalando el programa

Lo primero y más importante es descargarse el programa gratuito. Descárgatelo desde aquí: https://www.gpg4win.org/download.html Verás que te pide una ayudita como donativo. Yo les he echado una mano, pero si no puedes, no te preocupes, selecciona la opción 0$ y comenzará la descarga.

La instalación de Gpg4win es realmente sencilla, pero por si acaso voy a guiar tus pasos. Así nos aseguraremos de que todo irá bien cuando pasemos a la fase de gestión. Te pongo todos los pasos que verás al instalar. Realmente sólo tienes que pulsar el "siguiente".

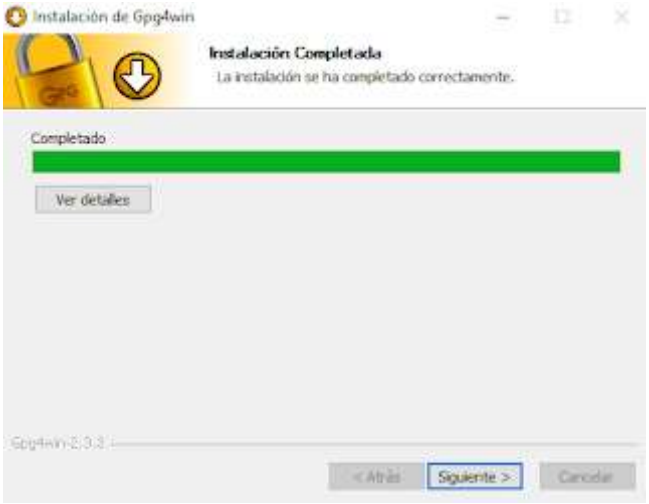

Instalación de Gpg4win
Selección de componentes
Seleccione qué características de Gpg4win desea instalar.
Marque los componentes que desee instalar y desmarque los componentes que no desee instalar. Presione Siguiente para continuar.
Seleccione los componentes a instalar:
GnuPG
Kleopatra
GPA
GpgOL
GpgEX
Gpg4win Compendium
Descripción
Sitúe el ratón encima de un componente para ver su descripción.
Espacio requerido: 95.2MB
Gpg4win-2.3.3
< Atrás
Siguiente >
Cancelar


Instalación de Gpg4win
Elegir lugar de instalación
Elija el directorio para instalar Gpg4win.
El programa de instalación instalará Gpg4win en el siguiente directorio. Para instalar en un directorio diferente, presione Examinar y seleccione otro directorio. Presione Siguiente para continuar.
Directorio de Destino
C:\Program Files (x86)\GNU\GnuPG
Examinar...
Espacio requerido: 95.2MB
Espacio disponible: 84.5GB
Gpg4win-2.3.3
< Atrás
Siguiente >
Cancelar


Instalación de Gpg4win
Opciones de instalación
Vínculos de inicio
Por favor seleccione dónde debe Gpg4win instalar los vínculos:
Menú inicio
Escritorio
Barra de inicio rápido
(Sólo las aplicaciones serán vinculadas en la barra de inicio rápido.)
Gpg4win-2.3.3
< Atrás
Siguiente >
Cancelar


Instalación de Gpg4win
Elegir Carpeta del Menú Inicio
Elija una Carpeta del Menú Inicio para los accesos directos de Gpg4win.
Seleccione una carpeta del Menú Inicio en la que quiera crear los accesos directos del programa. También puede introducir un nombre para crear una nueva carpeta.
Gpg4win
7-Zip
Accessibility
Accessories
Administrative Tools
Agencia Tributaria
Battle.net
Bonita BPM Community
Dropbox
ESET
FLAC To MP3
Games
Garmin
Gpg4win-2.3.3
< Atrás
Instalar
Cancelar


Instalación de Gpg4win
Elegir Carpeta del Menú Inicio
Elija una Carpeta del Menú Inicio para los accesos directos de Gpg4win.
Instalación de Gpg4win
Por favor asegúrese que otras aplicaciones no están ejecutándose. En especial, cierre Outlook y las ventanas del Explorador de Windows. Gpg4Win intentará instalarse de todas formas, pero será necesario que reinicie su sistema una vez terminado el proceso.
Aceptar
Gpg4win-2.3.3
< Atrás
Siguiente >
Cancelar


Instalación de Gpg4win
Instalación Completada
La instalación se ha completado correctamente.
Completado
Ver detalles
Gpg4win-2.3.3
< Atrás
Siguiente >
Cancelar

¡¡Muy bien!! ¡Ya lo tienes instalado!

Verás que en tu escritorio te ha aparecido un icono de un avatar femenino con el pelo rojo y que se llama Kleopatra. Éste es el programa de gestión que vamos a utilizar para generar tu clave pública y privada, así como guardar las claves públicas de aquellos compañeros analistas con los que quieras compartir información cifrada.

Ver video en el siguiente link:

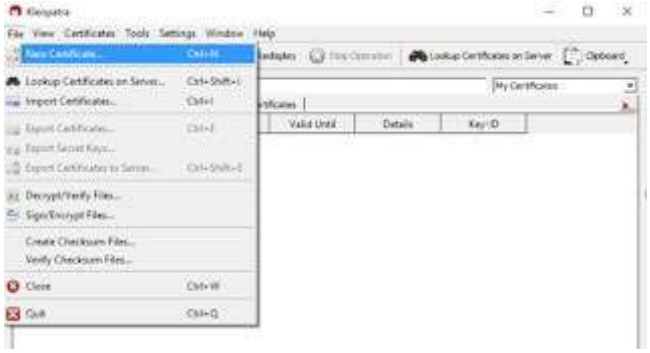
https://www.youtube.com/watch?v=ckf-rEiS3Ds
https://videos.pair2jeux.tube/videos/watch/dff01a95-4ea4-4755-85e4-100b9cfb2abe

ANEXO 3

MANUAL DE OPERACIÓN Y USO

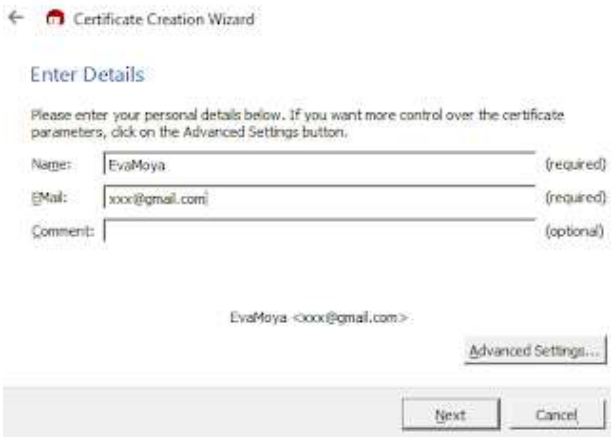
1. Creando nuestra clave pública y privada

Doble clic sobre el icono de Kleopatra y verás que se te abre la siguiente ventana. Ve a "File" y pulsa en "New certificate".



Lo siguiente que te pide es que decidas el tipo de certificado que quieres generar. Vamos a seleccionar el del OpenPGP:

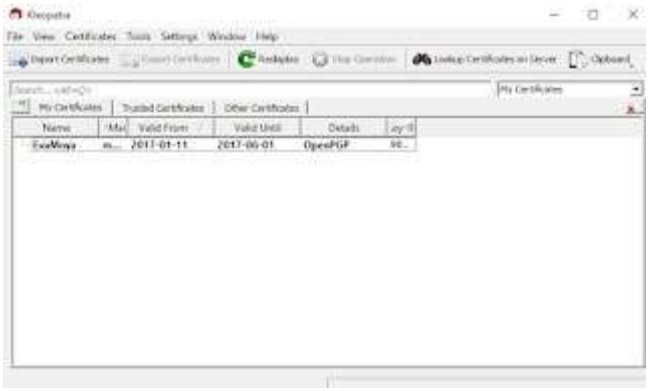
Tras pedirte que nos cree nuestro par de claves en OpenPGP, se abre el siguiente cuadro en el que debemos meter nuestro nombre y un email. En la pantalla hay una pestaña que te da la opción de ir a una configuración avanzada, "Advanced Settings". Pincha sobre este botón, verás que dejamos por defecto el cifrado en RSA. Lo que nos interesa es darle una validez concreta a dicha clave, es decir, una fecha de caducidad por motivos de seguridad. El mínimo recomendable suelen ser 6 meses, así que cambia las fechas al mínimo que consideres apropiado para ti:



Tras dar en "ok" se te abrirá un cuadro resumen con lo que has seleccionado. Si estás de acuerdo, pulsa en "Create Key". Al pulsar se te pedirá que des una contraseña de seguridad, que será la que te pida siempre que quieras descifrar algún mensaje, en definitiva, será tu clave privada. Verás que la barra de calidad te muestra si cumple con los criterios de seguridad. Procura que sea algo compleja, pero que puedas recordarla. De nada sirve que la tengas apuntada por ahí... ;-)

Una vez que lo hayas hecho y confirmado, verás que tu nueva clave asimétrica ya ha sido creada, con el siguiente mensaje. Te recomiendo que después, hagas una copia de seguridad por si tuvieras que restaurar el programa. La copia se hace en "Make a Backup". Simplemente guárdala en el directorio que especifiques:

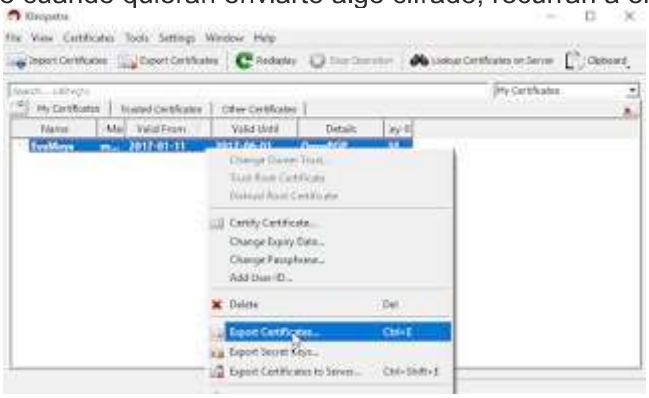
Tras hacer clic en "Finish", pasará ya al panel de control de las claves:



2. Pasarle nuestra clave pública a los compañeros con los que compartiremos la información cifrada.

Evidentemente los compañeros deben tener Kleopatra, así que ya sabes.

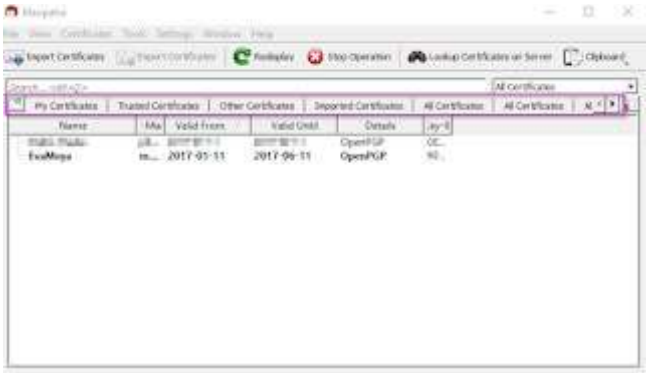
Es muy sencillo, seleccionas la clave que quieres compartir, botón derecho del ratón y opción "Export Certificates". Te la guardará por defecto en .asc. Ese será el ficherito que envíes a tus compañeros, para que cuando quieran enviarte algo cifrado, recurran a ella.



3. Importar la clave pública de nuestros compañeros.

Esto es tan sencillo que no necesita de captura. Simplemente pídeles que te envíen su clave pública. Le das al botón de "Import Certificates" buscas los .asc en la carpeta en que los hayas guardado y automáticamente te los carga en tu panel de control.

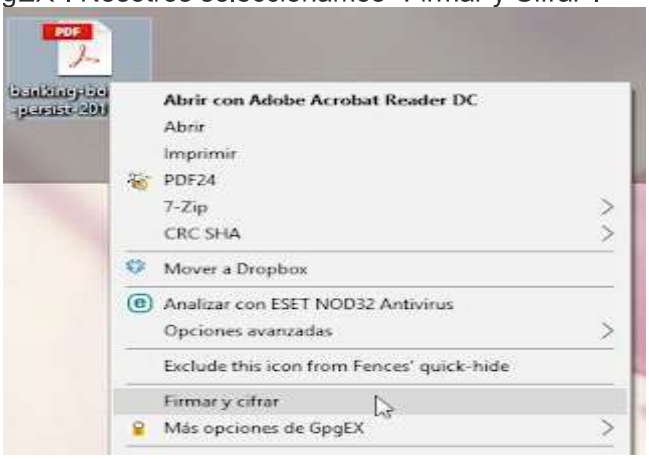
Es importante que una vez tengas el listado, te aparezca este pequeño menú de navegación que te remarco para que, si quieres, puedas ver todas las claves, es decir, la tuya y la de tus compañeros. Si no, sólo te mostrará la de tus compañeros por defecto. Para verlo todo es la opción "All certificates".



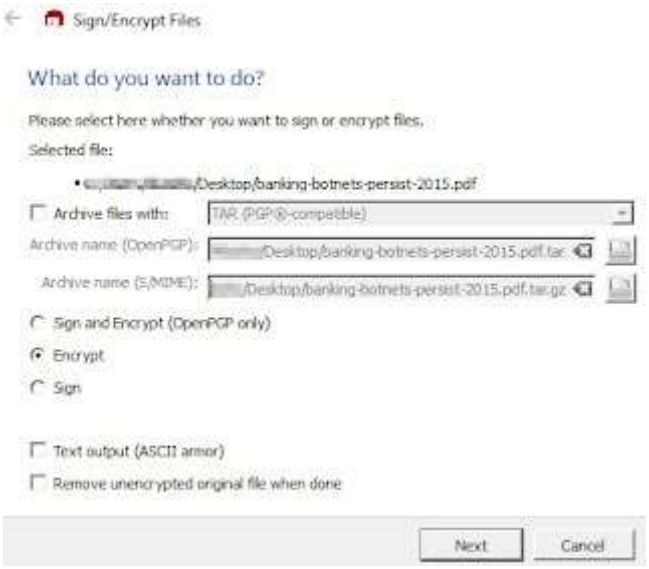
4. Cifrar un archivo con la clave pública del compañero al que queremos pasarle el archivo

Bien, ahora que ya tenemos todos los certificados que necesitamos, vamos a mandarle a nuestro compañero un archivo cifrado.

Lo primero es localizar el documento en nuestro ordenador. He pensado en enviarle a mi compi analista un informe sobre las botnets en el sector bancario. Para ello, hacemos clic en el botón derecho del ratón y observamos que tenemos dos nuevas funcionalidades. "Firmar y cifrar" y "Más opciones de GpgEX". Nosotros seleccionamos "Firmar y Cifrar".



En la siguiente pantalla simplemente respetamos por defecto lo que viene seleccionado y le damos a "Next".



Tras pulsar en "Next", se abre el cuadro de diálogo de la gestión de las credenciales para que decidas para cuáles de tus compañeros quieres cifrar el archivo. Puedes añadir todos los que quieras utilizando el botón "Add", y, recuerda añadirte a tí también por si quieres volver a descifrar dicho archivo ;-) Cuando ya tengas toda la lista, pulsa en "Encrypt".

Si todo ha ido bien saldrá una barrita de porcentaje y un mensaje como éste. Dale a "Finish":

Y aquí está el archivo cifrado. Como es interesante abrirlo para ver si lo ha cifrado realmente, lo he asociado al programa de win "bloc de notas", por eso me aparece con su icono. Pero no tienes por qué hacerlo si no quieres.

Lo importante es que vayas al archivo, pulses con el botón derecho y selecciones "abrir con". Selecciona el bloc de notas. Debería aparecerte algo como esto:

Pues ale, ya está listo para enviarlo a través de un email por la red, o incluso si lo prefieres, subirlo a un archivo compartido del tipo dropbox, drive, etc.

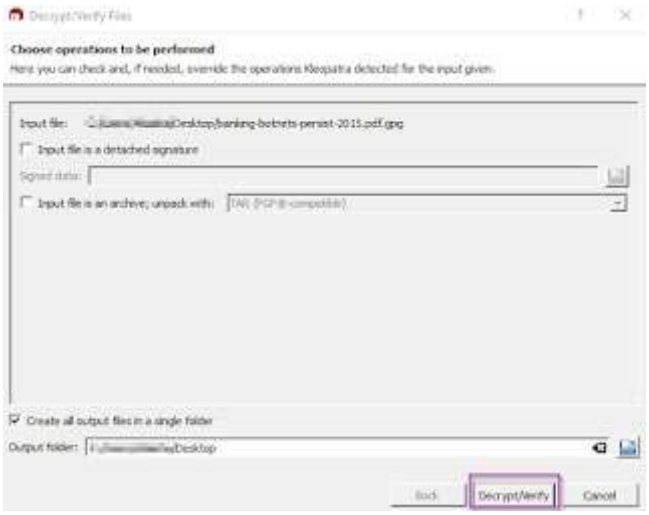
5. Descifrar un archivo cifrado con Kleopatra en el que nuestros compis han utilizado nuestra clave pública

Ahora vamos a realizar el proceso inverso. Supongamos que nos ha llegado este informe de botnets en la banca de 2015 vía email. Nos lo manda un compañero que ha cifrado el archivo con nuestra clave pública.

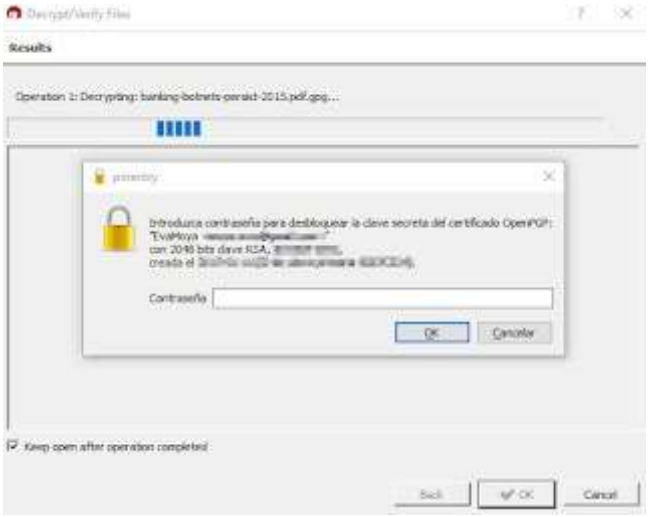
El proceso es muy sencillo.

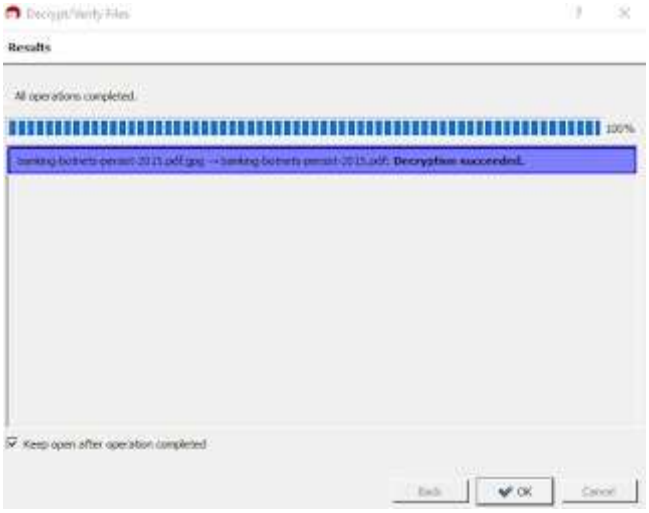
Lo primero es hacer clic en el botón derecho del ratón y seleccionar "Descifrar y Verificar":

Cuando lo hagas se abrirá la siguiente ventana en la que no tienes que tocar nada. Sólo dale al botón de "Decrypt/Verify":



¿Te acuerdas de que cuando configuramos tu certificado te pidió una contraseña? Pues este es el momento de meter tu clave privada, esa que sólo sabes tú:





¡Una vez que la introduzcas correctamente el documento ya debe haberse descifrado! Puedes comprobarlo en la ruta donde se te estén guardando (normalmente el escritorio).

Ver video en el siguiente link:

https://www.youtube.com/watch?v=ckf-rEiS3Ds
https://www.youtube.com/watch?v=4jVUcqJoTLI