

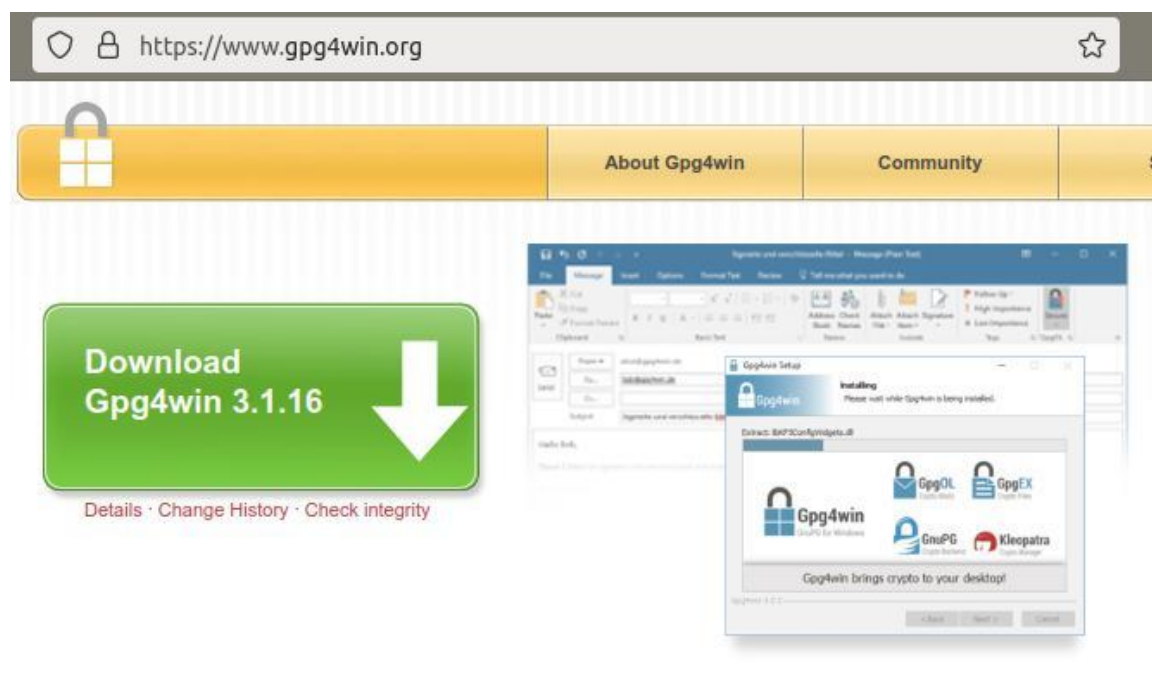
¿ Qué es GPG ?

Ver descripción [aquí](#)

GPG para usuarios windows

Existen varias aplicaciones bajo el sistema operativo Windows que permiten generar un par de claves gpg. Entre las más conocidas está **Gnu4win** y su módulo [Kleopatra]. La aplicación Gpg4win es un software de encriptación de libre distribución el cual permite el cifrado de ficheros y el envío de documentos a través del correo electrónico utilizando criptografía de clave pública para el cifrado de datos y firmas digitales.

Soporta los estándares de criptografía OpenPGP y S/MIME (X.509).

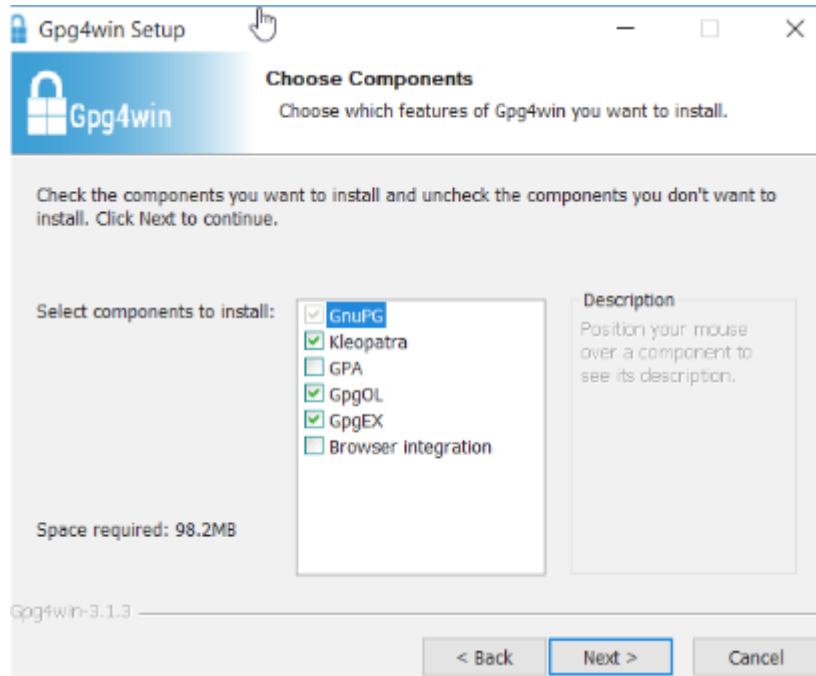


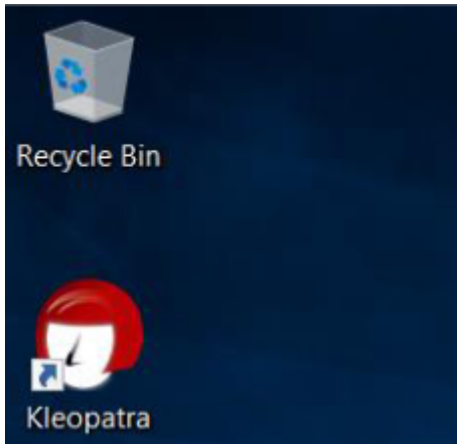
Gpg4win se compone varios módulos, entre ellos:

- GnuPG : la herramienta de cifrado básico
- Kleopatra : administrador de certificados para OpenPGP y X.509
- GPA : un administrador de certificados alternativa (GNU) para OpenPGP y X.509

Instalación de GPG4win

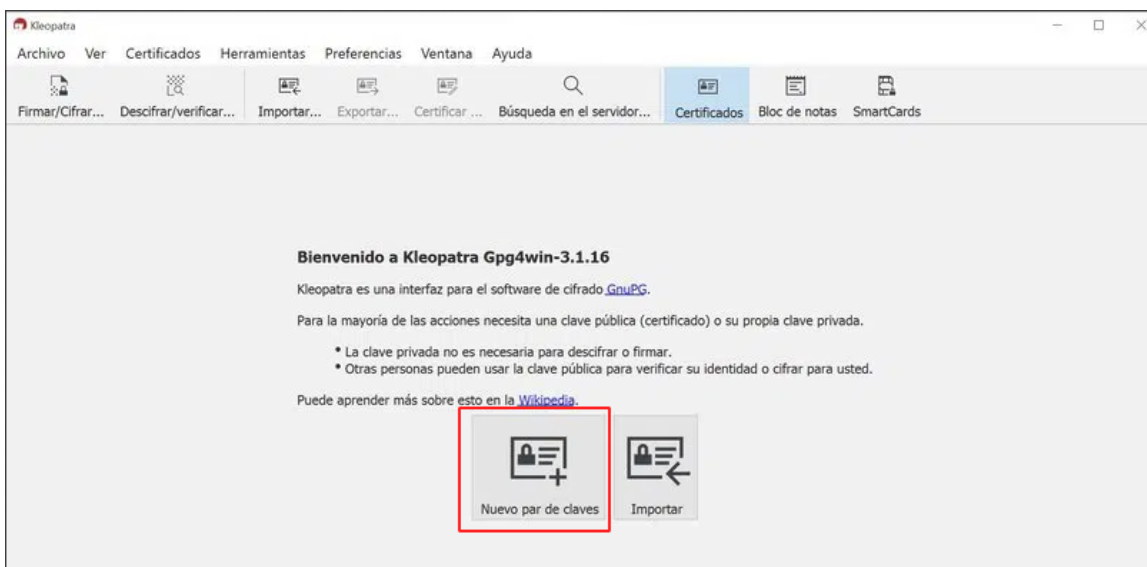
En la web del proyecto descargar la versión más reciente del software. Abrir el instalador y autorizar los cambios en caso necesario. Seguir los pasos indicados con el botón Siguiente.





Generar una par de claves (pública y privada)

Una vez instalado Gpg4win vamos a utilizar el módulo **Kleopatra** para generar un nuevo par de claves gpg. Para ello desde la pestaña *Archivo* seleccionamos *Nuevo Certificado*, lo cual abrirá el asistente de generación de certificados.



Pulsa en *Nuevo par de claves GPG*

Elegir formato

Por favor, elija qué tipo quiere crear.

- **Crear un par de claves personales OpenPGP**
Los pares de claves OpenPGP están certificados por la confirmación de la huella digital de la clave pública.
- **Crear un par de claves personales X.509 y una petición de certificación**
Los pares de claves X.509 se certifican por una autoridad de certificación (CA). La petición generada necesita enviarse a la CA para finalizar la creación.

Next

Cancel

Introducir los datos requeridos

? ×

Introduzca detalles

Por favor, introduzca sus detalles personales debajo. Si desea más control sobre los parámetros, pulse el botón «Configuración avanzada».

Nombre: (opcional)

Correo: (opcional)

Proteger la clave generada con una frase de contraseña.

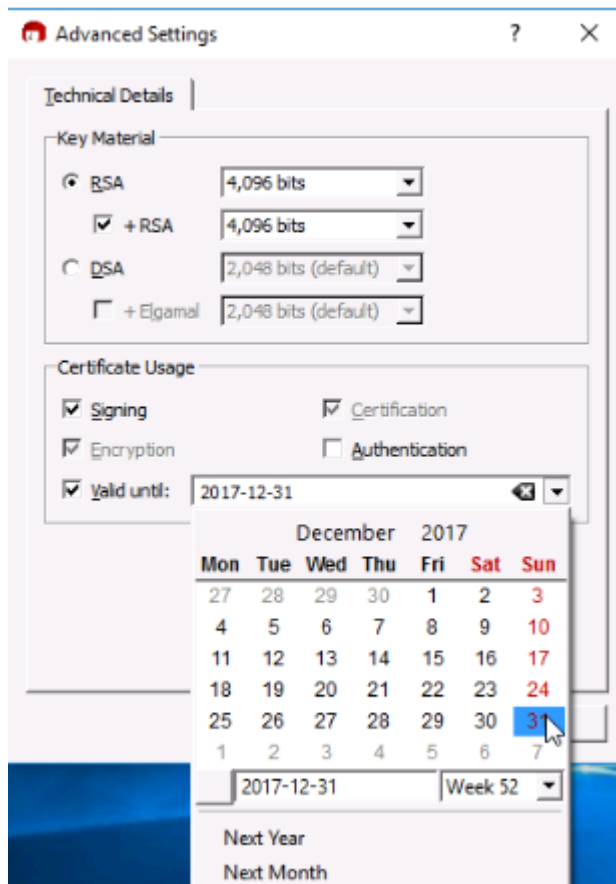
Julián G.

Configuración avanzada...

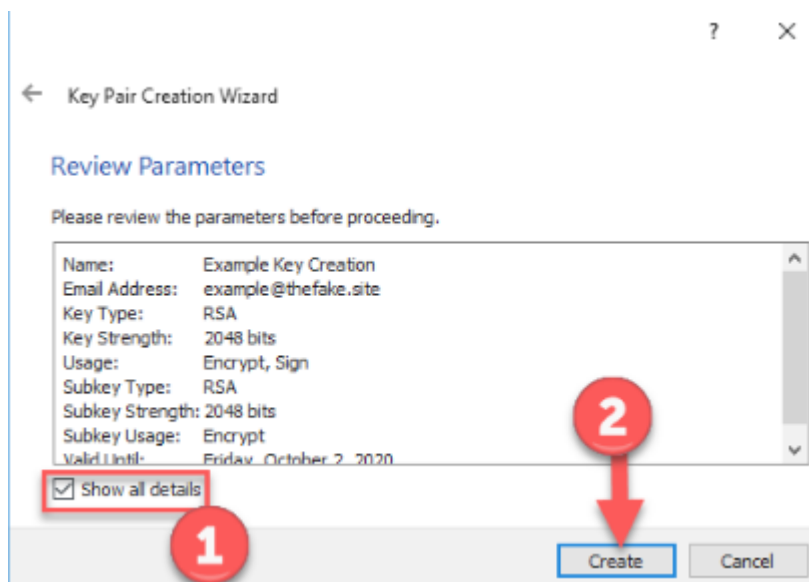
Crear

Cancel

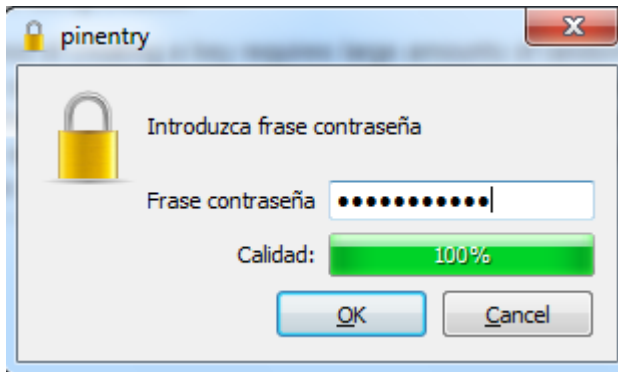
En la pestaña *Avanzadas* indicar una longitud de clave de 4096 bits y una fecha de caducidad en el desplegable inferior no superior a 2 años.



Confirmar los valores introducidos y generar las claves pulsando en *Crear*.



Introducir una contraseña que recuerde para su clave privada. Esta contraseña será la que deba usar para descifrar los archivos que reciba cifrados con su clave pública.



Al pulsar **OK** verá que su par de claves pública/privadas se han generado correctamente

← Asistente de creación del par de claves

Par de claves creado correctamente

Su nuevo par de claves se ha creado correctamente. Consulte los detalles sobre el resultado y algunos pasos a seguir sugeridos más abajo.

Resultado

Par de claves creado correctamente.
Huella digital: 0A97759CC84026BD56749920AB4FBBA7E0C0E342

Siguientes pasos

Hacer copia de respaldo de su par de claves...

Enviar clave pública por correo...

Enviar clave pública a un servicio de directorio...

Finish

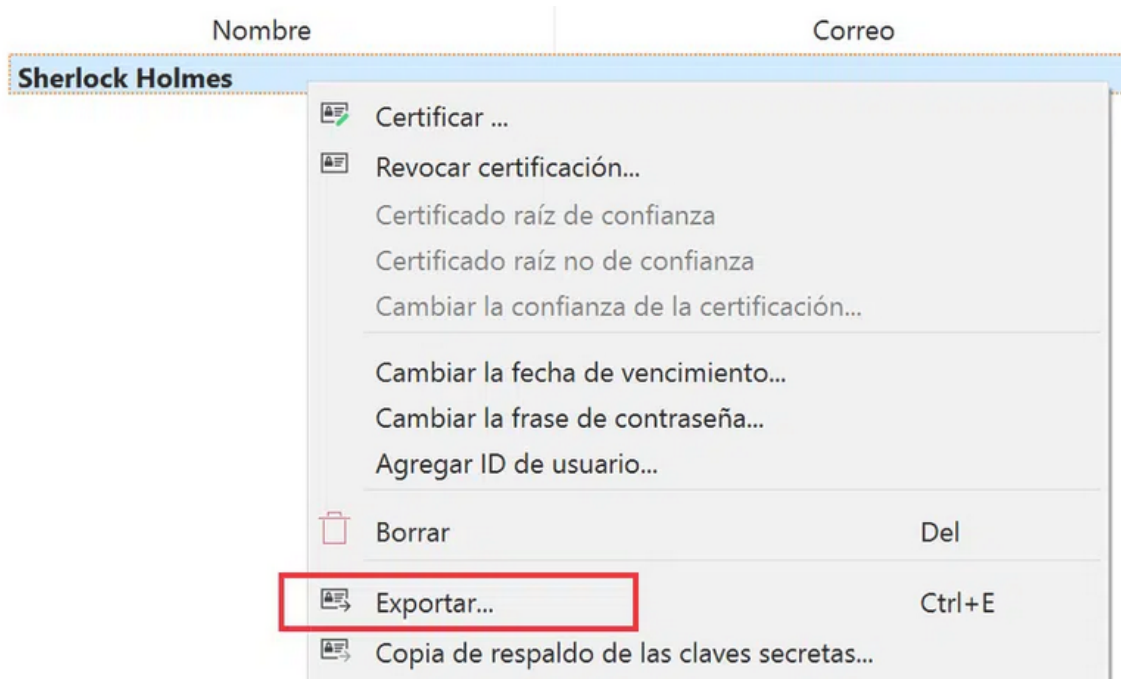
Cancel

Se puede comprobar que se han creado con éxito el par de claves en la pestaña *Certificados*.

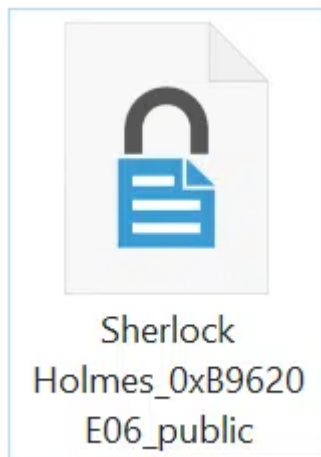


Exportar la clave pública

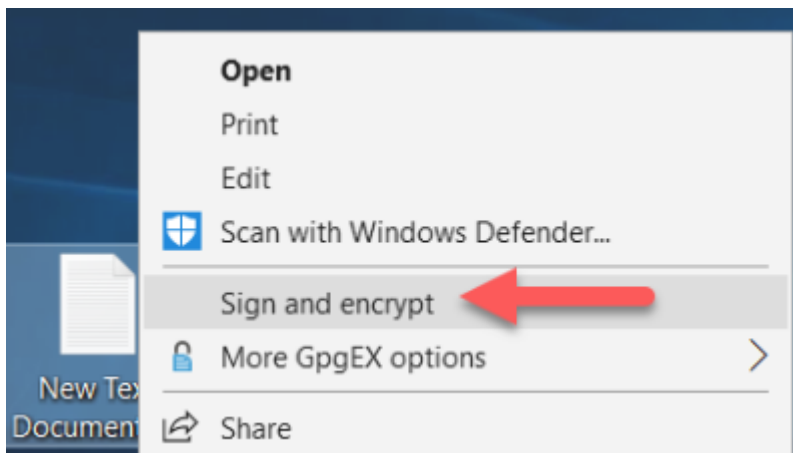
Al exportar la clave pública se genera un fichero de texto que por norma general se almacena con la extensión *.asc*, que es el que podrá distribuir por correo electrónico o bien **publicar en un servidor de claves públicas** como *REDIRIS* y donde cualquier persona la puede descargar.



Obtendrá un fichero de este tipo:



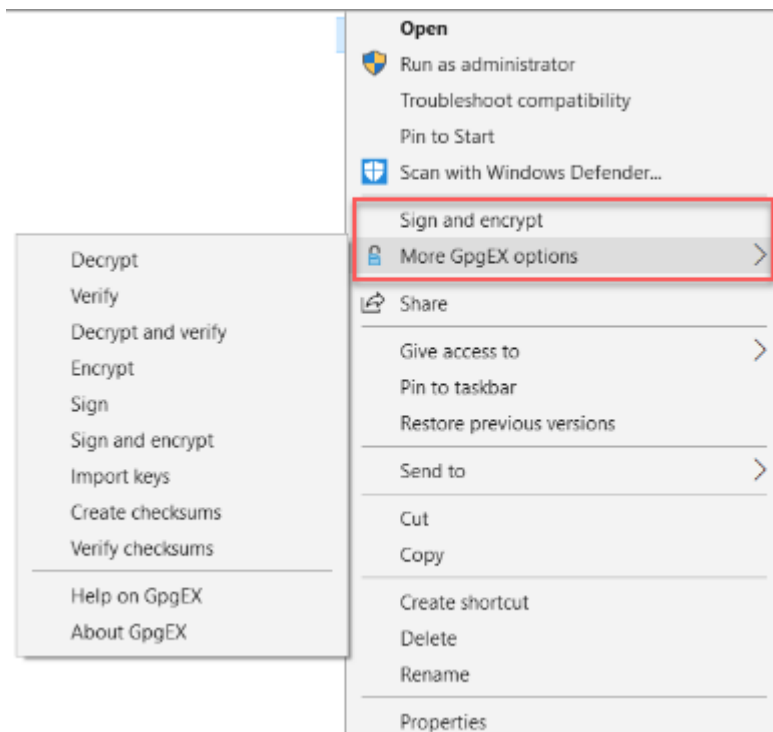
Cifrar ficheros con la clave pública.



Descifrar ficheros con la clave privada

Sólo si un archivo *.gpg* ha sido cifrado con su clave pública y tiene la clave privada, así como su contraseña, podrá descifrar su contenido.

Se puede usar el menú contextual *Descifrar y verificar* para recuperar el fichero original pulsando con el segundo botón. También es posible realizar esto desde Kleopatra.



Una vez descifrado este tendrá el mismo nombre sin la extensión *gpg*.

Todas las operaciones terminadas.

100%

TOP SECRET.docx (1).gpg → TOP SECRET.docx (1):

[Mostrar registro de auditoría](#)

Firma válida por **Dr. Watson**

Firma creada en viernes, 16 de julio de 2021 22:01:36

Con certificado:

[Dr. Watson \(9111 B0CB F48D C6DD\)](#)

La firma es válida y la validez del certificado es totalmente confiable.

NOTA IMPORTANTE: Si cambia de ordenador o usa uno diferente asegúrese de tener su par de claves a buen recaudo. Sin ellas no tendrá la posibilidad de descifrar el contenido del archivo. Por ello recomendamos realizar un backup del par de claves GPG