Encriptación de correos electrónicos con GnuPG (GPG) y OpenPGP

Publicado el El Informatico - 12 de diciembre de 2020 -

Si queremos mantener un nivel de privacidad elevado, además de encriptar las conexiones que realizamos a través de internet, que es el medio a través del cuál nos comunicamos, en ocasiones es importante encriptar también el contenido que compartimos en el mismo. Como, por ejemplo los correos electrónicos. En éste artículo se explica el funcionamiento del estándar **OpenPGP**, usado para cifrar los mensajes de correo electrónico.

Pretty Good Privacy (PGP)

PGP es un programa de encriptación desarrollado en 1991 que sirve para cifrar las comunicaciones y verificar la autenticidad y el origen de las mismas. Se basa en un protocolo de clave pública, donde las partes de la comunicación intercambian sus claves públicas para cifrar el contenido, intercambiarlo, y después desencriptarlo usando sus claves privadas.

Consta de los siguientes elementos:

- **Huella PGP**: La huella PGP es un hash que se usa para identificar una clave pública. Ésta huella es compartida entre las partes de la comunicación para averiguar qué clave pública le corresponde a cada parte.
- **Claves pública y privada**: Son las claves que se usan durante el cifrado del contenido. La clave pública se intercambia entre los recipientes del mensaje, mientras que la privada se mantiene en secreto.
- **Servidor LDAP**: Son servidores que utilizan un protocolo (LDAP) con el cuál se almacenan y distribuyen las claves públicas y sus huellas PGP a través de todo internet.
- **Firma digital**: Es un componente opcional que permite firmar los mensajes para verificar su procedencia. Para ello, se utiliza una **clave simétrica**.
- **Red de confianza (Web of trust)**: Es un concepto sobre cómo verificar que las firmas digitales sean de confianza. En la actualidad esto se consigue mediante usuarios que, siendo de confianza, otorgan esa confianza en dicha clave. Generalmente las claves se generan e intercambian en persona (en el

mundo físico), para verificar su procedencia.
- **Certificados**: Las versiones más modernas pueden utilizar un **sistema de certificados digitales**, parecidos a los usados en TLS o SSL, para verificar la procedencia de las firmas y las claves mediante autoridades (CA), reemplazando así la red de confianza.

OpenPGP

OpenPGP es un estándar basado en el programa PGP original. Dado que PGP era un programa propietario (actualmente es propiedad de Symantec), y para evitar problemas con las patentes, la IETF (Internet Engineer Task Force) desarrolló el nuevo estándar OpenPGP como alternativa libre a PGP. Este es el estándar que se usa normalmente en Internet.

En la actualidad existen diversas implementaciones de éste estándar. La más común es GnuPG (GPG para abreviar).

Los problemas de PGP

PGP ha sido objeto de numerosas críticas. Las principales críticas son hacia su **complejidad de uso**. Mucha gente no está dispuesta a generar y mantener claves en un servidor, y renovarlas a mano al caducar. Además, su verificación es algo compleja. Las claves son largas y complejas, y su uso es también algo complejo.

Naturalmente a lo largo de los años han surgido numerosas vulnerabilidades que se han ido subsanando con el tiempo mediante nuevas versiones del estándar, lo que hace que mensajes que se cifraran hace años con una versión más antigua ya no se puedan volver a descifrar en una versión más moderna. Lo que además implica que los clientes tengan que verificar la versión del estándar que usa cada uno durante la comunicación.

Por éstos motivos, se están buscando alternativas a éste estándar, aunque todavía no se ha encontrado el reemplazo perfecto.

¿Es seguro?

El estándar OpenPGP es criptográficamente seguro, siempre que se utilice la última versión del mismo. Pero dado que en ocasiones se encuentran vulnerabilidades, **los mensajes que se hayan mandado con una versión anterior podrían ser descifrados por un tercero con el tiempo**. Eso quiere decir que un mensaje que mandes hoy con la última versión no podrá ser descifrado hoy, pero tal vez en cinco años alguien sea capaz de descifrarlo usando alguna vulnerabilidad encontrada para la última versión.

Encontrar vulnerabilidades en el protocolo no es tarea sencilla, pueden pasar muchos años hasta que se descubra una vulnerabilidad seria en el protocolo. Pero

es una posibilidad. En cualquier caso, tampoco es tarea sencilla almacenar datos durante periodos de tiempo extremadamente largos, por lo que es muy complicado que alguien descifre tus mensajes ya que, para entonces, probablemente habrán perdido el interés o el mensaje ya ha perdido su valor, o simplemente el mensaje se haya perdido en el tiempo (si, por ejemplo, lo borras del servidor).

Esto es sólo de importancia en el caso de que queramos ocultar datos que pudieran comprometernos a nosotros o a nuestra empresa. Como documentos gubernamentales o cosas así de serias. Desde el punto de vista de la privacidad (que por ejemplo "gmail" no lea nuestros correos) es totalmente seguro, y su uso es incluso recomendable.

Cómo usar OpenPGP o GnuPG

Para poder usar OpenPGP para encriptar nuestros correos necesitamos una clave pública y privada, almacenadas en un servidor LDAP, la huella de nuestra clave pública, y un cliente de correo que soporte PGP o un gestor de claves que incorpore dicha funcionalidad. En la página oficial de OpenPGP existen algunos ejemplos de clientes que soportan éste estándar, bien de forma nativa o mediante algún plug-in. Si preferimos usar la implementación GnuPG, en su página oficial también hay herramientas para ello.

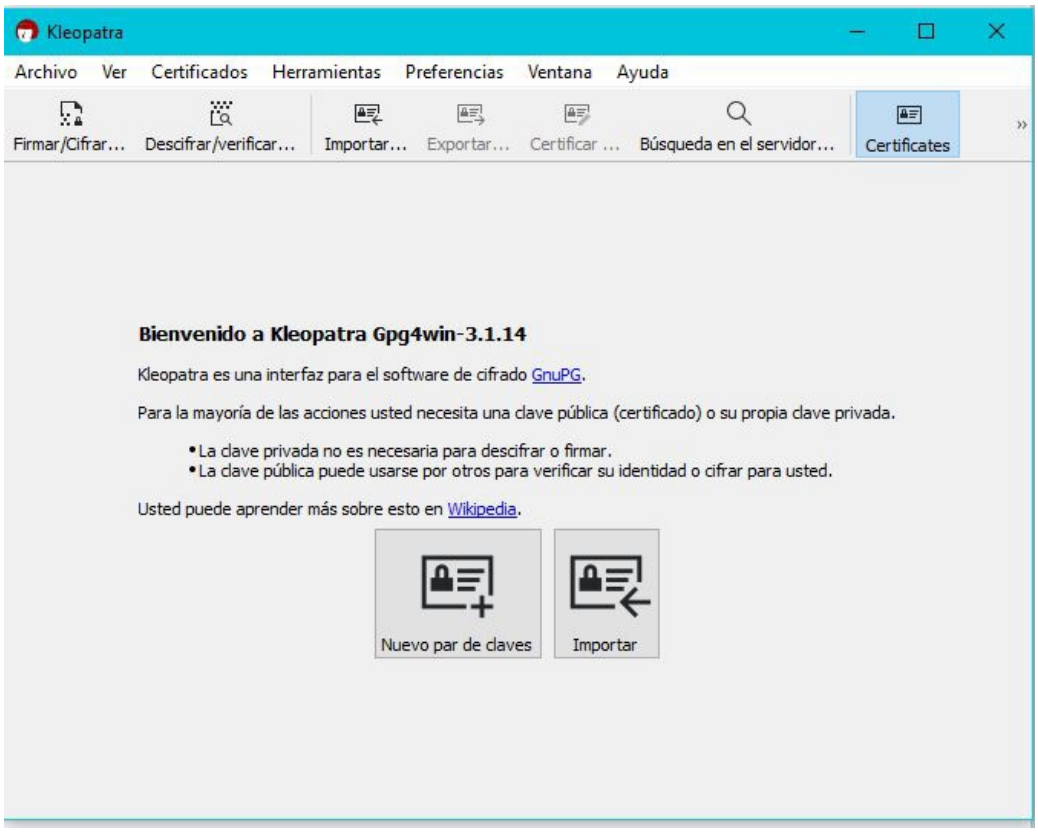
Si sólo queremos usar OpenPGP, Mozilla Thunderbird tiene incorporado por defecto soporte para éste estándar. Por el contrario, para usar GnuPG es necesario de plug-ins adiccionales tanto para éste gestor como para Outlook.

GnuPG en Windows: Gpg4win

Si queremos usar GnuPG en Windows, podemos hacerlo mucho más fácilmente a través de Gpg4win. Es un conjunto de aplicaciones y extensiones open source, entre las que se incluyen Kleopatra, GPA, GpgOL (para Outlook), y GpgEX, para la generación y gestión de claves y la encriptación y verificación de mensajes usando GnuPG, así como plugins para el navegador.

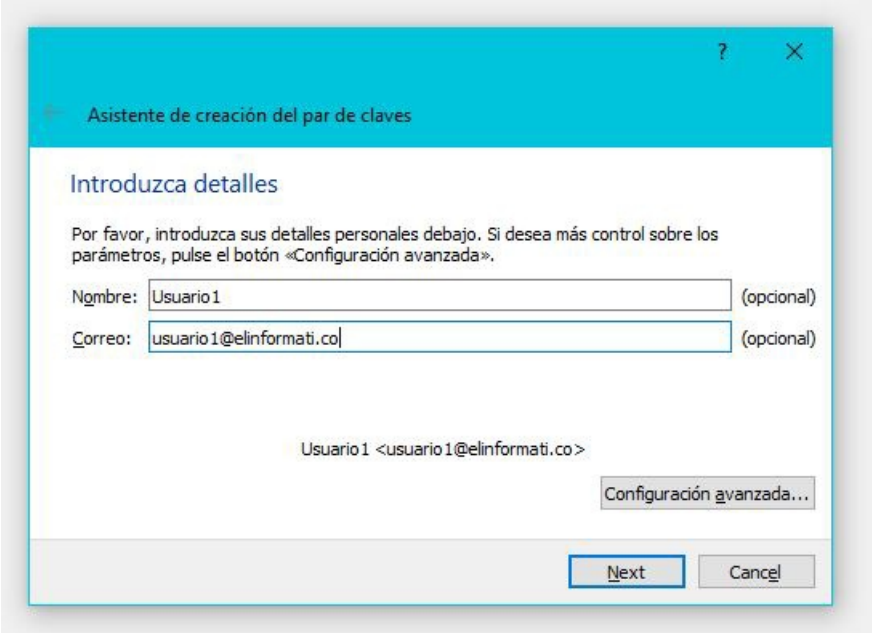
Su instalación es muy sencilla, basta con ejecutar el instalador que descargamos desde la página de **Gpg4win con permisos de administrador** como cualquier otra aplicación.

Usando Kleopatra



Gestor de claves Kleopatra

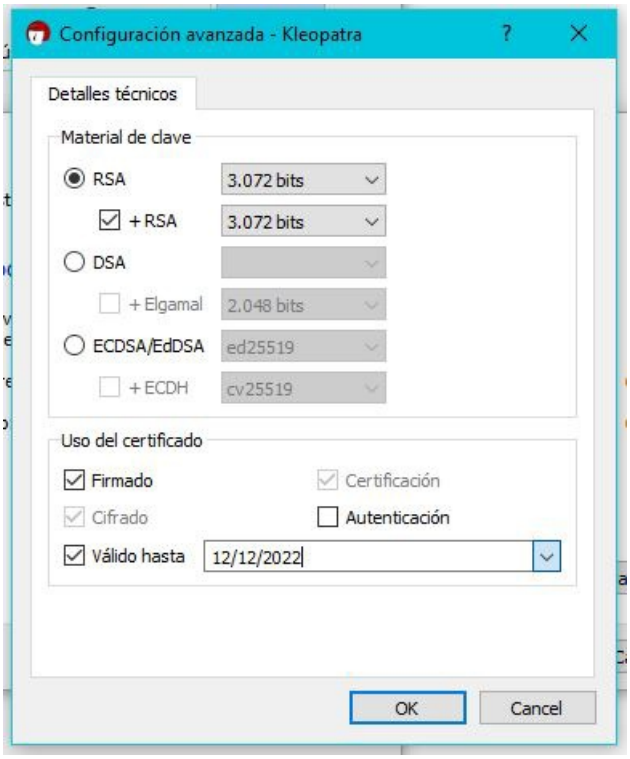
Kleopatra es el gestor de claves y certificados por defecto para GnuPG. Si es la primera vez que ejecutamos el programa, nos permitirá **generar un nuevo par de claves, o importar claves ya creadas**. Si no dispones de un par de claves entonces deberás empezar por crear un nuevo par haciendo click sobre **nuevo par de claves**.



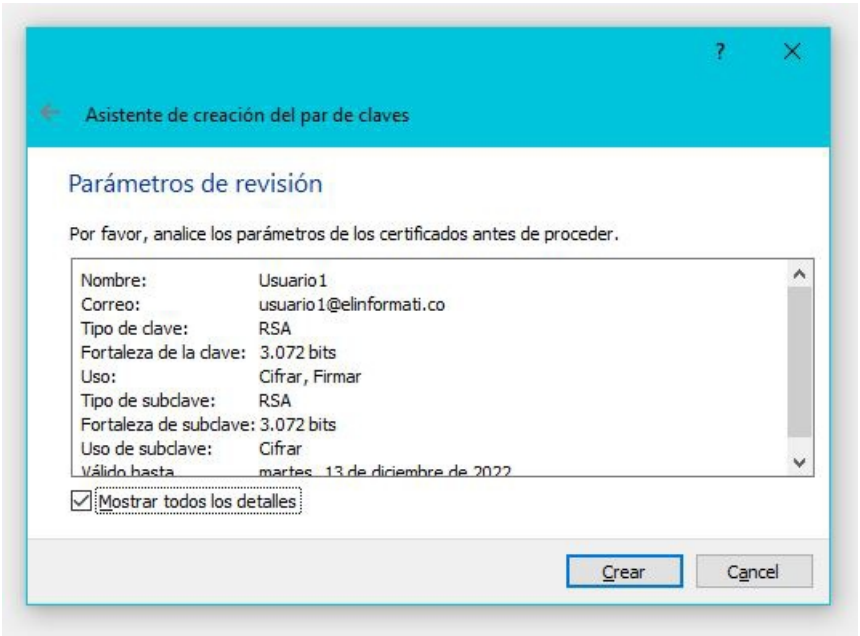
Al iniciar el asistente, deberás escribir un nombre para la clave (Por ejemplo, tu nombre, para así certificar que esa es tu clave), y el correo con el que vas a usarlo.

Las claves se configurarán con la configuración por defecto. La clave será válida durante un año, y el algoritmo de cifrado usado será RSA de 3072 bytes. Si lo

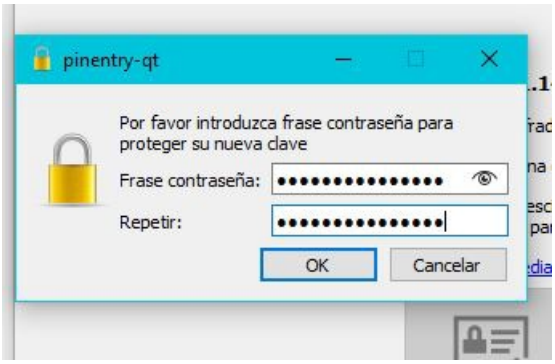
necesitaras, puedes cambiar éstos parámetros en **Configuración avanzada**.



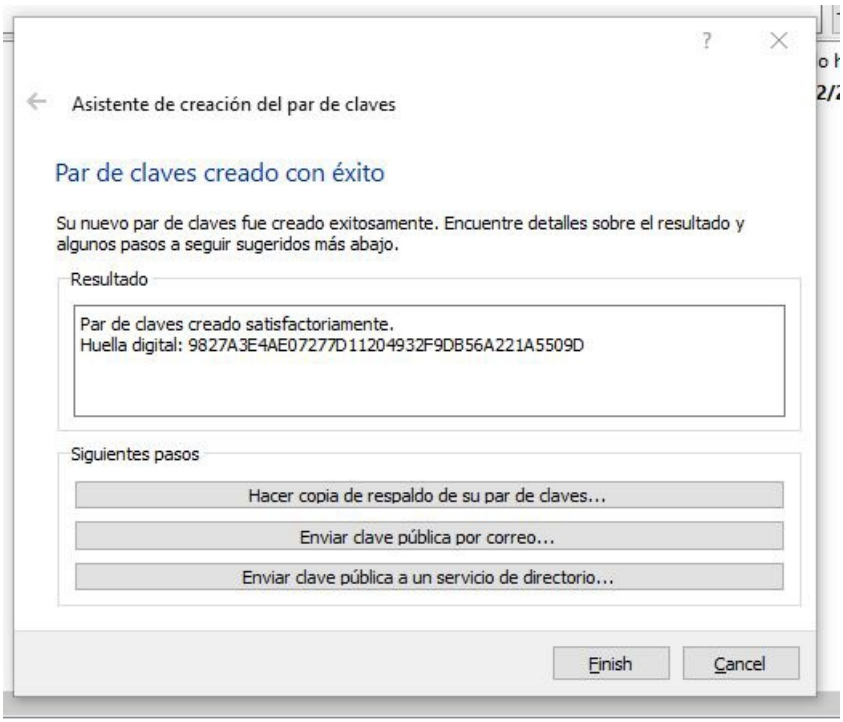
No obstante, esto es opcional y con los valores por defecto debería ser suficiente. Para ir al siguiente paso, hacemos click en Next, donde se muestra un resumen de los parámetros especificados para la clave.



Si estás conforme con éstos parámetros, haz click en **Crear**. Para generar la clave, será necesaria una contraseña. Kleopatra nos pedirá una contraseña que deberemos especificar cada vez que queramos encriptar o desencriptar el mensaje. Ésta contraseña **debería ser segura**, conteniendo al menos 8 caracteres, con una mezcla de caracteres alfanuméricos y símbolos (Como @, $, guiones, etc).



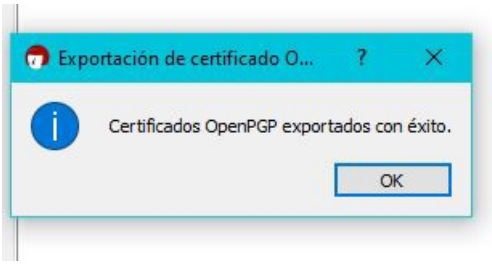
Una vez tengas la contraseña, haz click sobre **OK** para finalizar el asistente. Aparecerá una pantalla con tu **huella digital**. Esa huella digital es el identificador de tu clave, así que anótala bien ya que la gente con la que mandes correos encriptados te la solicitará para poder descargar tu clave.



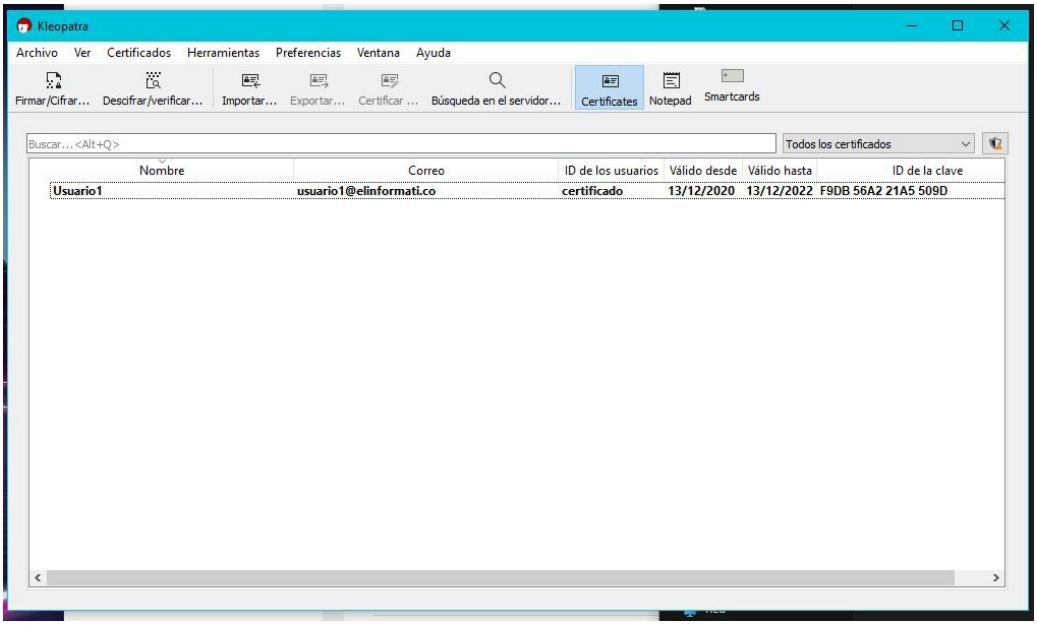
El siguiente paso es subir la clave pública a los servidores LDAP. Kleopatra te lo pone fácil, ya que sólo tienes que hacer click en el botón **Enviar clave pública a un servicio de directorio**, y el programa lo subirá automáticamente.

El programa te pedirá que te asegures de que tengas un certificado de revocación en caso de que quieras borrar la clave. Si has seguido el asistente, éste se genera por

defecto, así que ignora el mensaje y haz click en **Continuar**. Espera unos segundos a que se suba el certificado.

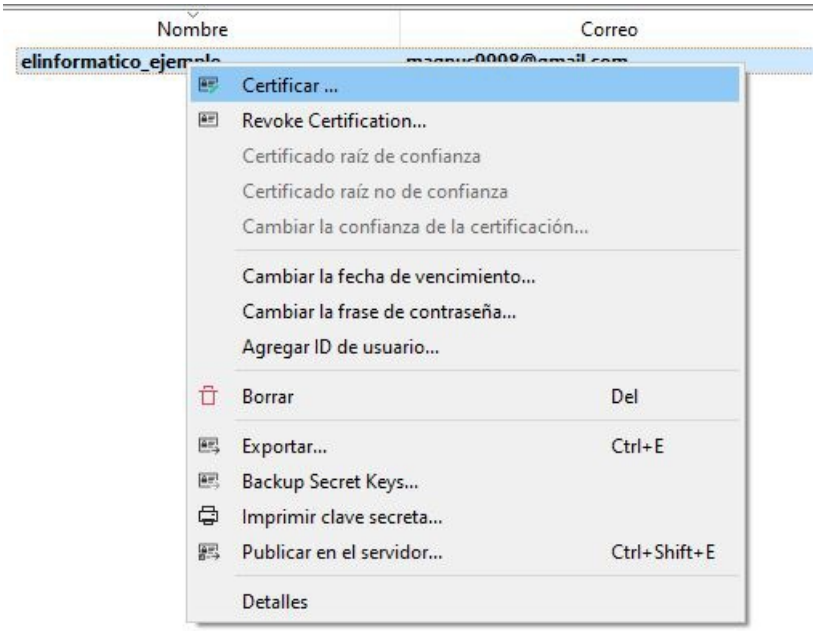


Una vez subido a internet, Kleopatra te lo notificará con un mensaje. Al finalizar, volverás a la interfaz principal de Kleopatra, donde puedes gestionar todas las claves que hayas generado o descargado.



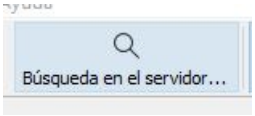
Gestión de claves con Kleopatra

Podemos gestionar cualquier clave que hayamos creado o descargado con Kleopatra haciendo click sobre la clave con la que queremos interactuar.

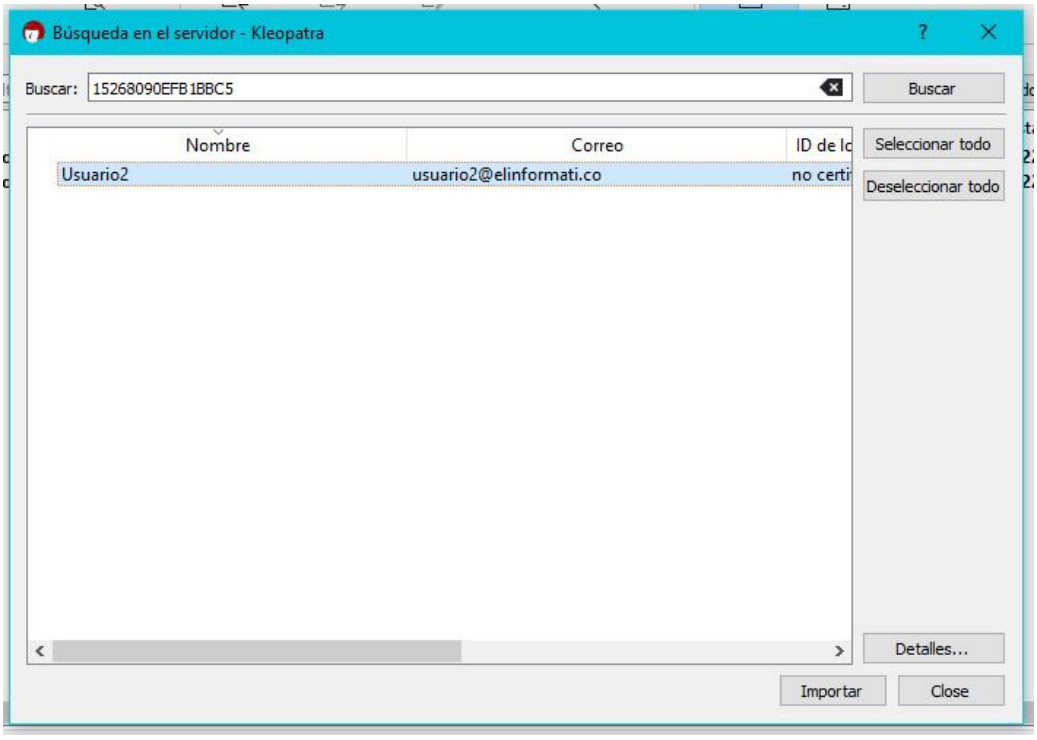


Podemos **certificar que una clave es válida si queremos ser parte de una red de confianza**, **revocar un certificado** (si disponemos del certificado de revocación) **si queremos anular la clave**, cambiar la fecha o la contraseña de la clave, exportarla, subirla a un servidor LDAP, etc.

Si queremos mandar un correo encriptado, primero necesitamos la clave del recipiente o recipientes a los que queremos mandar el correo. Si disponemos de ellas, podemos importarlas con el botón **Importar**. O podemos buscarlas haciendo click en **Buscar en el servidor**.



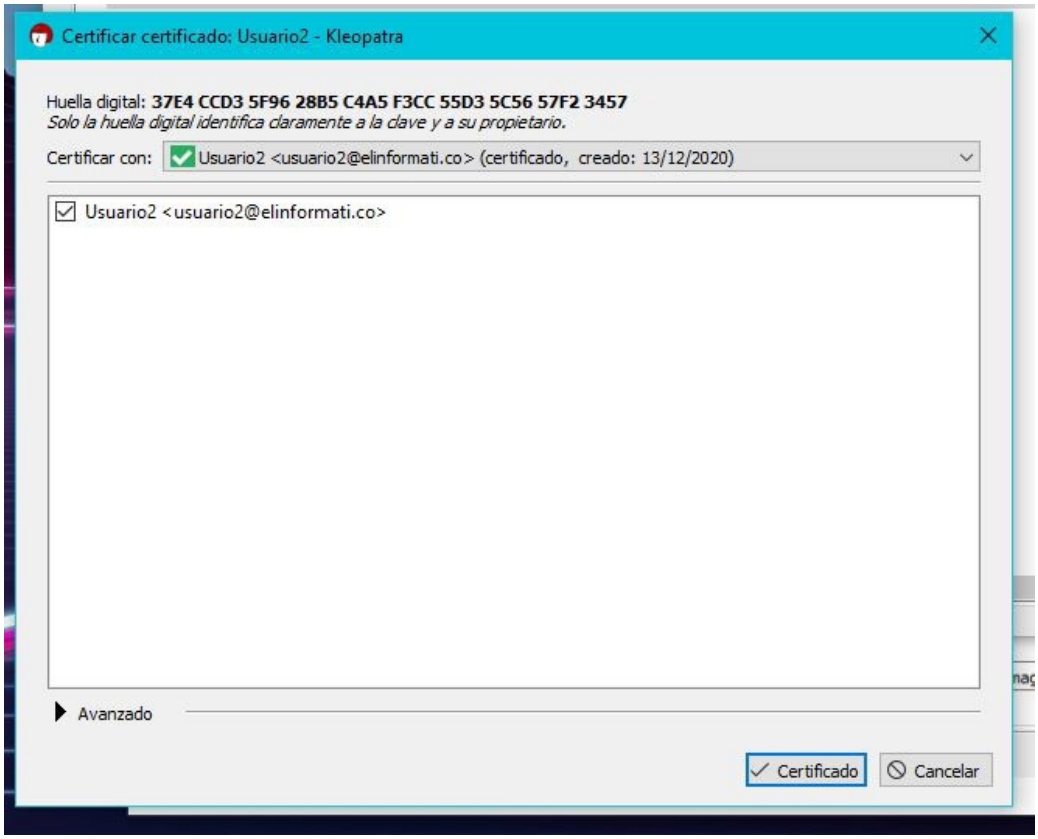
Al realizar una búsqueda, se puede realizar una búsqueda **usando la huella, por nombre, o por correo**. Solo tienes que introducir uno de éstos valores en el campo de búsqueda y hacer click en el botón **Buscar**. Si hay resultados, se mostrarán en una lista en la ventana de búsqueda.



Para añadir cualquiera de los resultados a nuestra lista de claves, sólo debes hacer doble click sobre la clave que estés buscando. También puedes importar varias claves al mismo tiempo seleccionándolas y pulsando sobre el botón **Importar**.

En cualquier caso, el programa nos ofrece la posibilidad de **certificar la validez de las claves al importarlas**.

Si quieres ser parte de una red de confianza, haz click en **Sí**, y certifica las claves que quieras seleccionándolas de la lista.



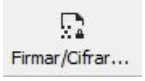
Al finalizar, las claves aparecerán en la lista de la interfaz principal.

Cifrar el correo

Los correos cifrados con GnuPG no son más que correos con un archivo de texto cifrado adjunto a los mismos. Para conseguir esto, tenemos dos vías:

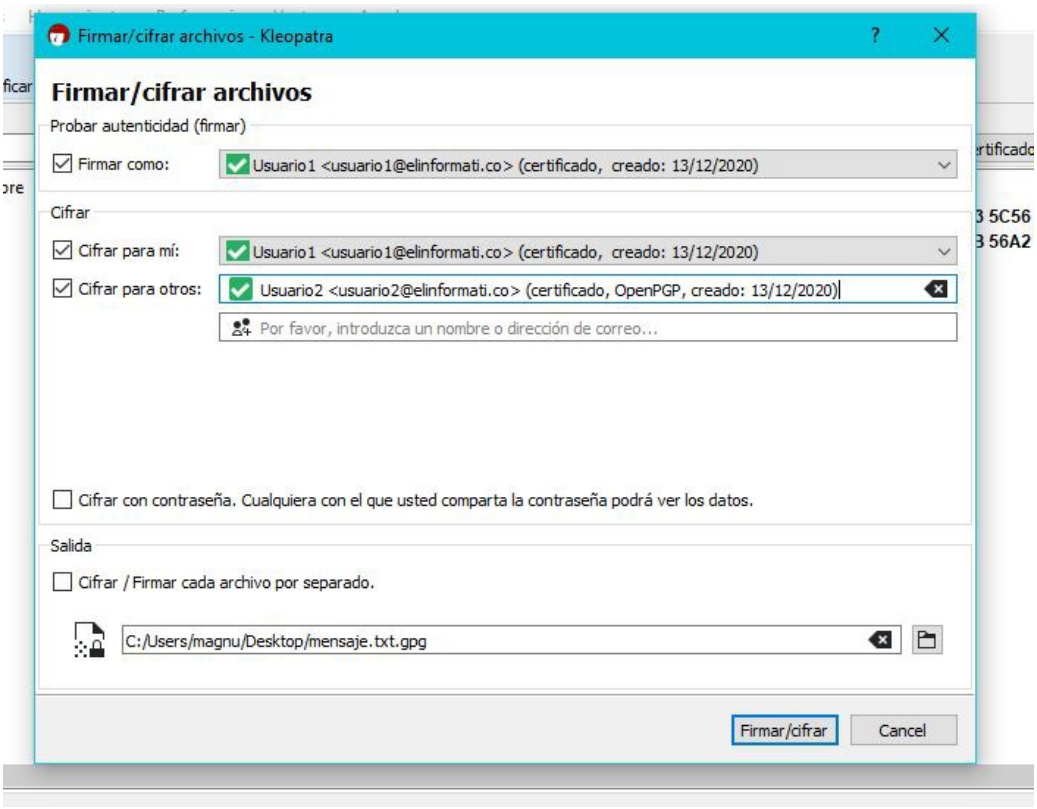
1. **Cifrar un archivo de texto con Cleopatra y adjuntarlo con tu correo**.

Puedes cifrar cualquier archivo usando la opción **Firmar/Cifrar**.



Kleopatra te pedirá que selecciones el archivo que quieres cifrar. Una vez

seleccionado, aparece una pantalla donde deberás especificar si quieres cifrarlo para ti, o si quieres cifrarlo para otra persona. Para hacer esto, **deberás tener la clave del destinatario en tu lista, y que además ésta esté verificada**. Para mandarlo a otra persona, selecciona "Cifrar para otros", **y establece el o los nombres de los destinatarios**.



NOTA: Deberás seleccionar a la vez las opciones de "Cifrar para mí" y "Cifrar para otros" si quieres poder visualizar el mensaje con tu clave, además de la del destinatario. Si sólo marcas "Cifrar para otros", sólo el destinatario podrá visualizarlo.

Al pulsar sobre **Firmar/cifrar**, el programa te pedirá la **contraseña para tu clave** (la que especificaste al crearla). Introdúcela y pulsa sobre **OK**. Se generará un archivo PGP en el directorio de salida especificado.

Sólo tienes que adjuntar ese archivo a tu correo. El recipiente deberá después descifrarlo.

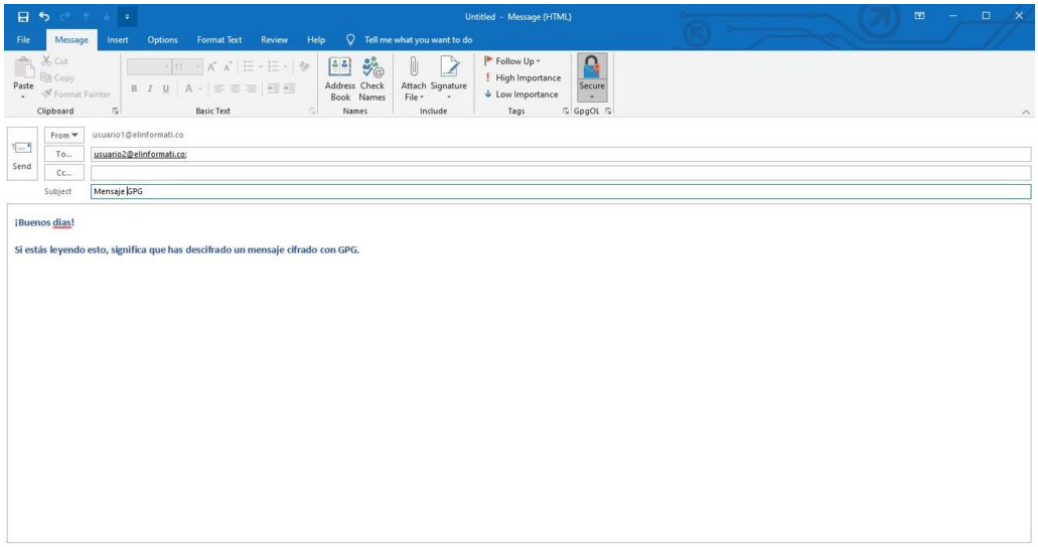
2. Directamente desde tu gestor de correo

Si lo quieres hacer desde tu gestor de correo, los pasos varían dependiendo del gestor que utilices. Si usas Outlook en Windows, Gpg4win incluye una extensión para Outlook llamada GpgOL que incorpora ésta funcionalidad.

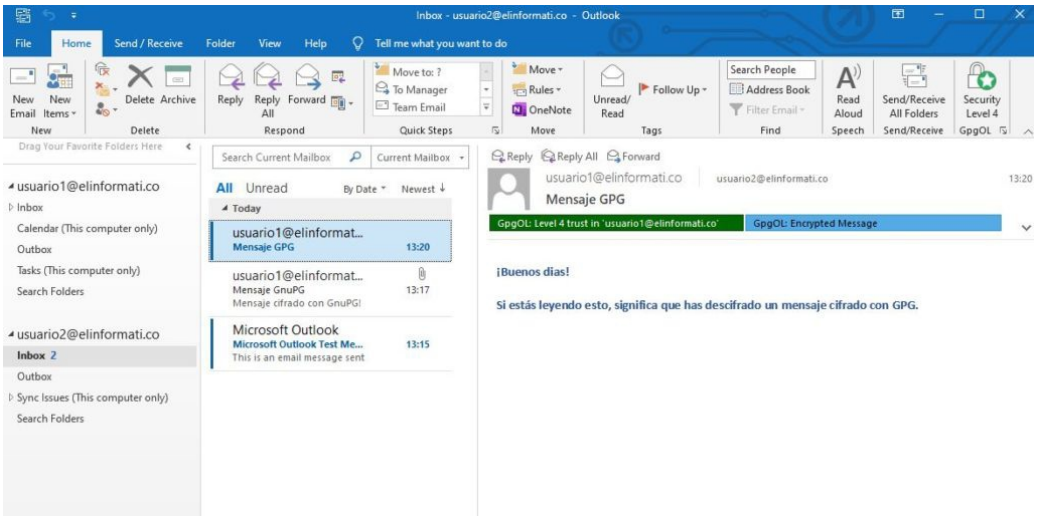
Al instalarlo, al crear un nuevo correo en Outlook, dispondrás de una nueva opción en el menú Mensaje.

Las dos opciones que nos permite son **firmar** y **encriptar**. Puedes seleccionar una o ambas opciones si lo deseas. No aparecerá ningún menú, sino que las opciones que selecciones se activarán.

Una vez activadas, redacta tu mensaje como normalmente lo harías, y haz click en **Enviar**.

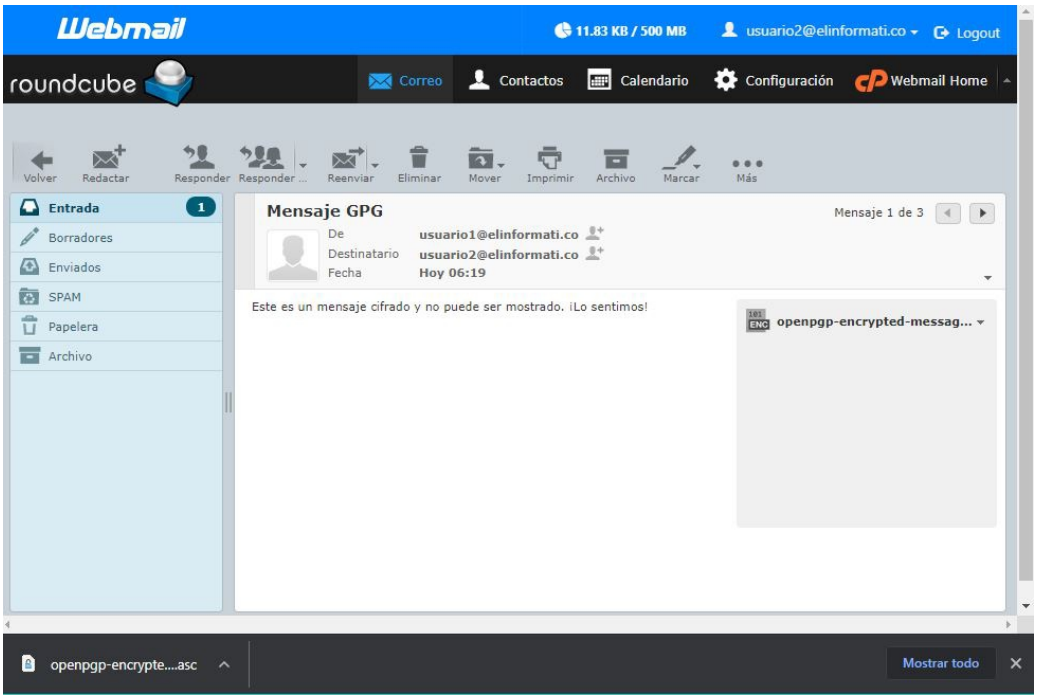


GpgOL te pedirá tu contraseña (la que especificaste al crear tu clave). Pulsa OK cuando la tengas, y el mensaje se enviará con el contenido ya cifrado y/o firmado.



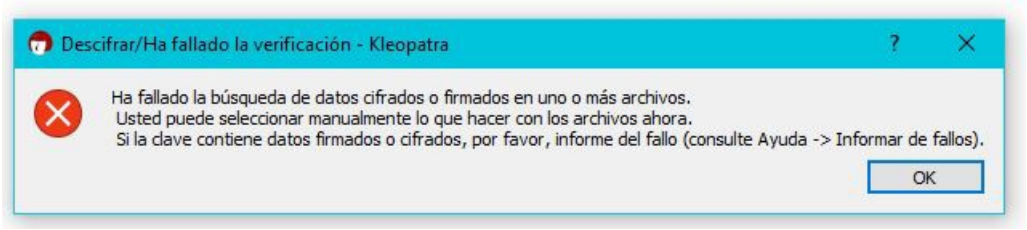
Descifrar el contenido

Si estás usando un gestor de correo, el miso se encargará de automatizar el proceso. Es decir, si tienes la clave del emisor, lo descifrará automáticamente. Pero si quieres descifrar el contenido de un mensaje, sólo tienes que descargar los adjuntos y desencriptarlos con **Kleopatra**.

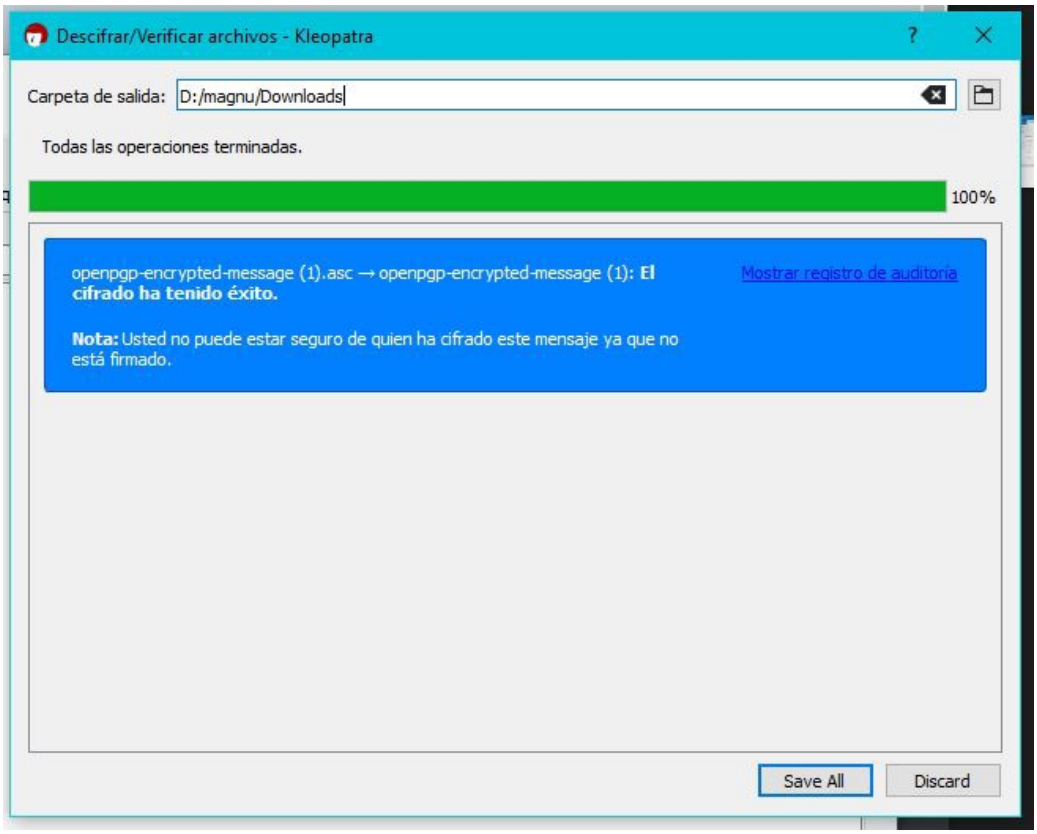


En Kleopatra, pulsa sobre el botón Descifrar/Verificar, y selecciona el o los archivos encriptados (con extensión asc o gpg dependiendo del método usado y el cliente). El archivo noname contiene la versión utilizada.

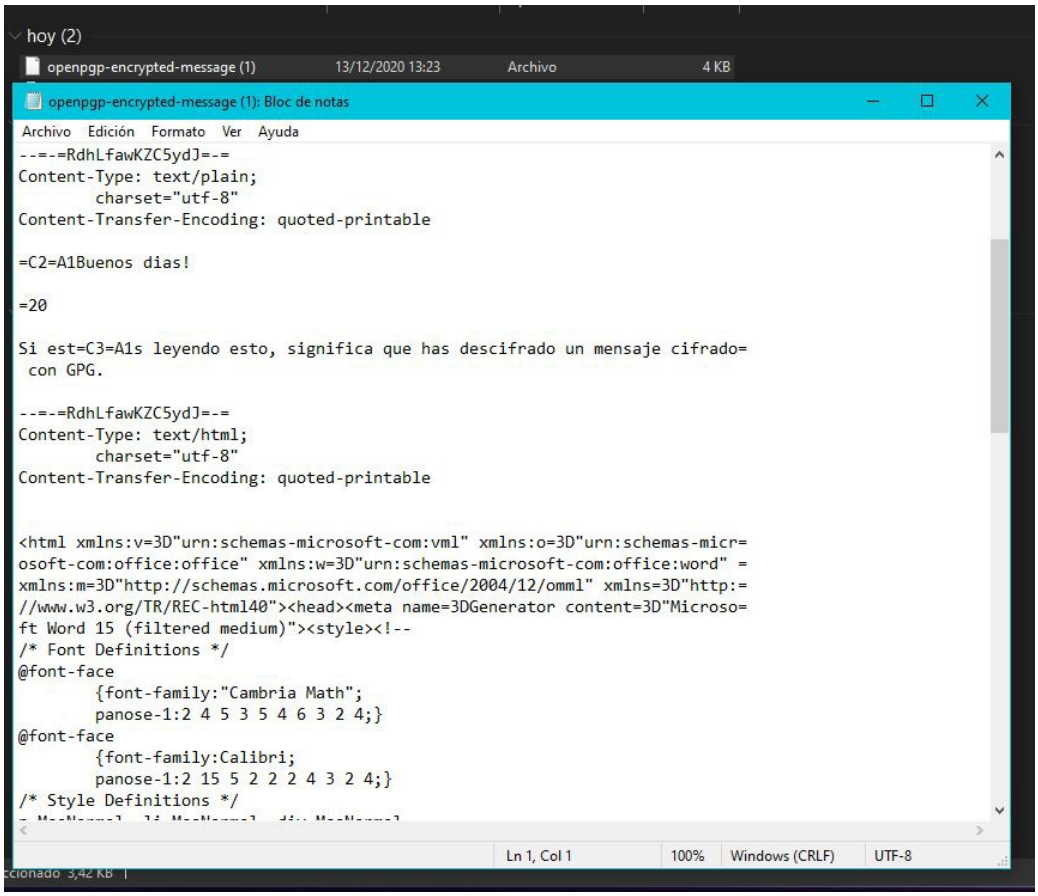
Asumiendo que ya tengas las claves del emisor descargadas, el proceso será automático. En caso contrario, mostrará un error y te pedirá que selecciones las claves adecuadas.



En cualquier caso, una vez finalize el proceso, aparecerá la siguiente ventana:

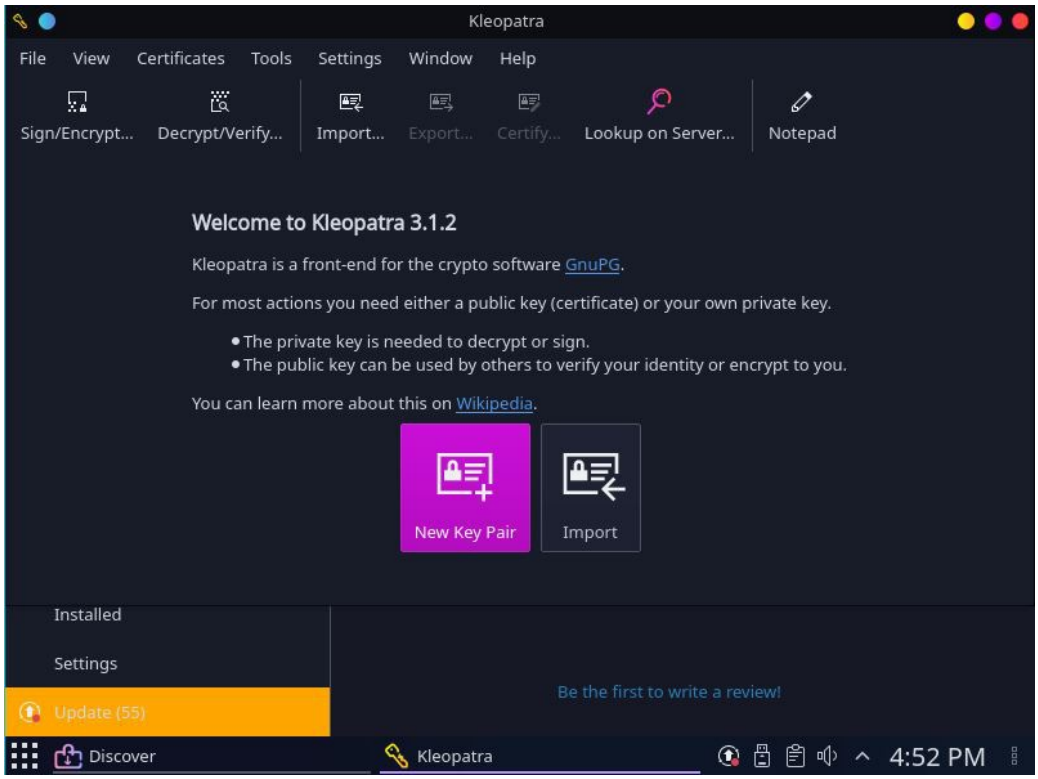


Haz click en **Save All** para guardar los archivos ya desencriptados en la **carpeta de salida**. Simplemente ábrelos con el programa adecuado. Por ejemplo, para mensajes de texto, con un editor de texto como el bloc de notas.



En Linux

Si quieres usar GnuPG en Linux de manera sencilla, Kleopatra está disponible para Linux en todas las distribuciones populares. Los pasos a seguir para usarlo son los mismos que para Windows, ya que es el mismo software.



A la hora de usar un gestor de correo que soporte GnuPG, **Thunderbird** es un cliente de correo electrónico que incluye soporte nativo para **OpenPGP**, pero

necesitarás una extensión llamada **Enigmail** si lo quieres usar con **GnuPG**. Dicha extensión se puede instalar desde los repositorios oficiales de Ubuntu o Arch bajo el nombre **enigmail**.

sudo apt install enigmail

En cualquier caso, siempre puedes adjuntar los archivos GPG de Kleopatra y desencriptar los descargados con el mísmo.

Android

En Android se puede usar una combinación entre k9mail y OpenKeychain. Tienen una versión en la PlayStore, pero recomiendo usar F-Droid o incluso **descargar e instalar los APK a mano para mayor seguridad**.

ANTERIOR

Malware, Virus informáticos y mecanismos de defensa

SIGUIENTE

Gestor de aplicaciones F-Droid para Android

Actualidad | Android | Básicos | Ciberseguridad | Criptografía | Emulación / Virtualización | FOSS | Hacking | Informática | Internet | Juegos | Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS