TEMA 2: Administración de credenciales de acceso a sistemas

Requisitos

Para la realización de las prácticas utilizaremos una máquina virtual con Ubuntu server sin entorno gráfico y una máquina virtual con Windows 10 o nuestro propio ordenador con sistema operativo Windows.

Práctica 2.4: GNUPG/Kleopatra

¿Qué es GNUPG?

Se trata de una implementación de fuentes abiertas del estándar PGP (OpenPGP).

Algunas características:

- Encriptar y firmar datos y comunicaciones.
- Gestión de claves.
- Acceso a directorios de claves públicas.
- Interfaz de comandos
- Soporte para Shell seguro (ssh).
- Frontend.

Emplear encriptación ayuda a proteger nuestra privacidad y la privacidad de nuestros interlocutores. Hace más dificultosa la tarea de espionaje de terceras partes.

Debido a restricciones legales no se permite bajar material criptográfico desde servidores localizados en EE.UU. a los no residentes en este país. Por esta razón PGP se encuentra siempre disponible en dos versiones: una internacional y otra para los EE.UU.

Instalación de GnuPG en Windows

La implementación para Windows de GnuPGP se llama GPG4Win. Tenemos disponible la descarga de la herramienta en la siguiente url:

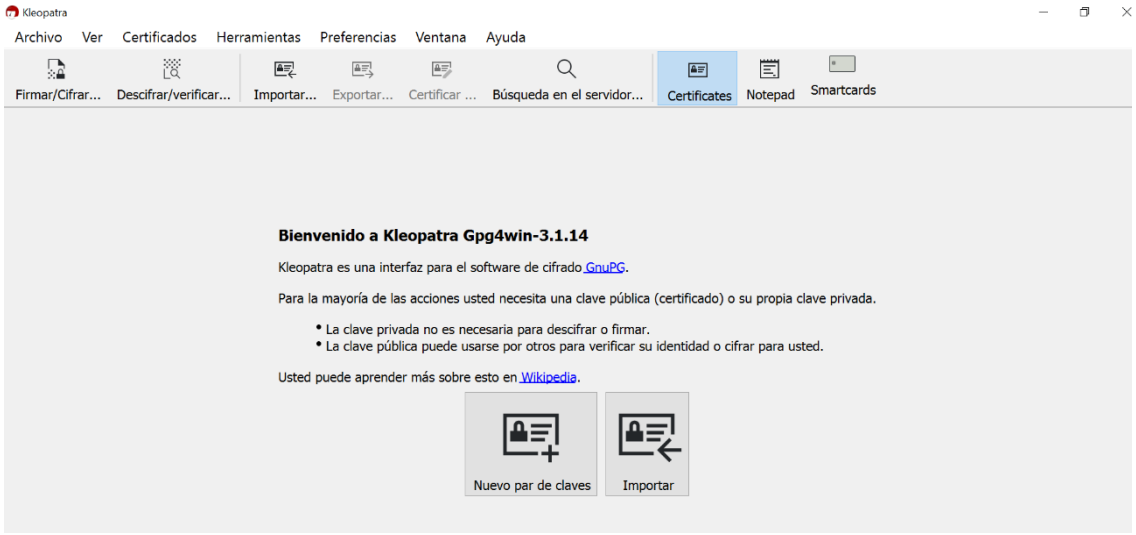
https://www.gpg4win.org/download.html

Pulsamos sobre el botón verde “GPg4win” y nos aparecerá la pantalla para donar y descargar el programa.

Para descargar el programa sin donar dinero, marcamos $0 y procedemos a descargar el ejecutable.

Descargamos el fichero y procedemos a la instalación de todos los componentes.

Cuando finaliza la instalación abrimos la herramienta Kleopatra recién instalada que maneja la implementación sobre Windows de GNUPG.

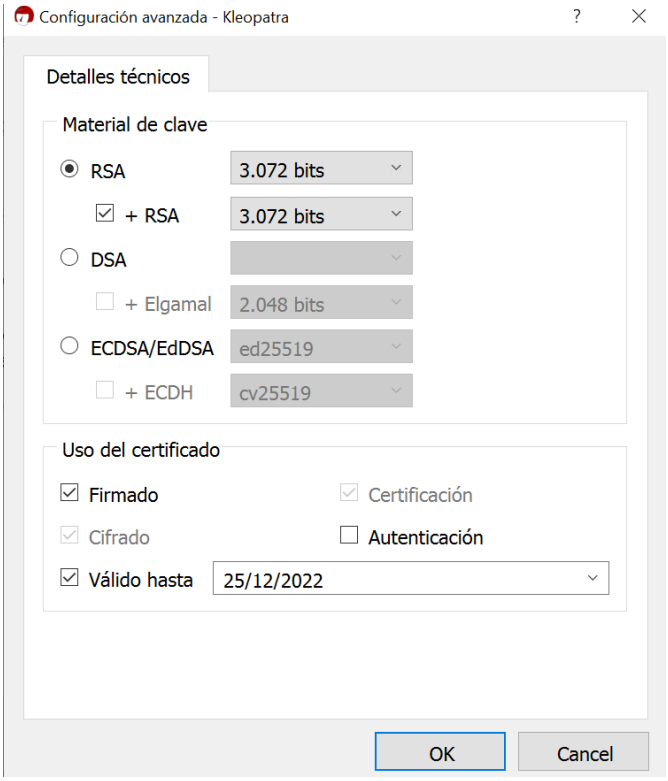


Creación de un certificado personal en kleopatra

Antes de crear un certificado personal, crearemos una carpeta donde almacenarlo. El certificado dispondrá de la funcionalidad de firmas y cifrar.

Para crear el certificado pulsaremos sobre el botón “Nuevo par de claves”

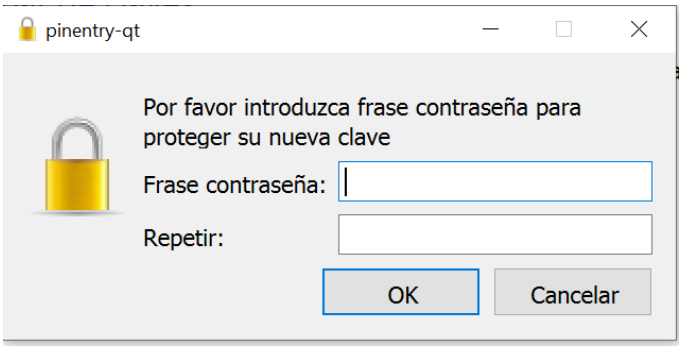
Rellenamos los campos Nombre y correo electrónico y pulsamos sobre “Configuración avanzada” para ver las opciones.



Vemos que podemos modificar el tipo de cifrado, los usos del certificado y la fecha de validez del mismo.

Vamos a dejar todos los parámetros por defecto y continuamos con el asistente.

Para finalizar pulsamos sobre el botón “Crear” y nos saltará una pantalla donde nos pide meter una contraseña para proteger la clave privada del certificado.



Vamos a hacer una copia de respaldo del par de claves y la guardaremos en una carpeta.

Kleopatra nos mostrará el certificado generado.

Operativa de kleopatra

1. Detalles de un certificado personal en kleopatra
2. Exportar la clave pública en Kleopatra
3. Exportar la clave privada en Kleopatra

La clave privada no se envía a nadie. Simplemente, haremos una copia de seguridad.

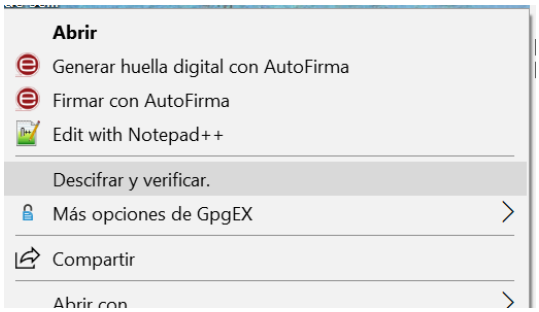
4. Importar una clave pública en Kleopatra

Partiremos de una clave pública que nos han enviado. Seleccionamos el archivo y con el botón derecho del ratón pulsamos sobre “Mas opciones de GpgEX”-> “Importar claves”.

5. Cifrar un archivo en Kleopatra

6. Descifrar un archivo en Kleopatra

La opción a seleccionar es “Descifrar y verificar”.



Necesitaremos poner la contraseña del certificado.

7. Obtener la firma de un archivo en Kleopatra

Obtendremos la firma asociada a un fichero. Necesitaremos el certificado que generamos anteriormente y el fichero del que vamos a obtener la firma.

En este caso cogeremos un fichero y procederemos a firmarlo pulsando con el botón derecho del ratón sobre el fichero y seleccionando “Firmar y cifrar”.

En este caso solamente seleccionaremos Firmar en las opciones que aparecen.

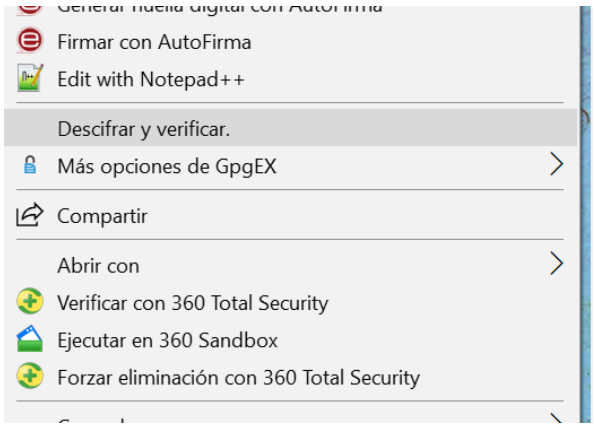
Al final obtendremos un fichero .sig que contendrá la firma del fichero.

Si abrimos el fichero obtenido vemos que está encriptado.

8. Verificar la firma de un archivo en Kleopatra

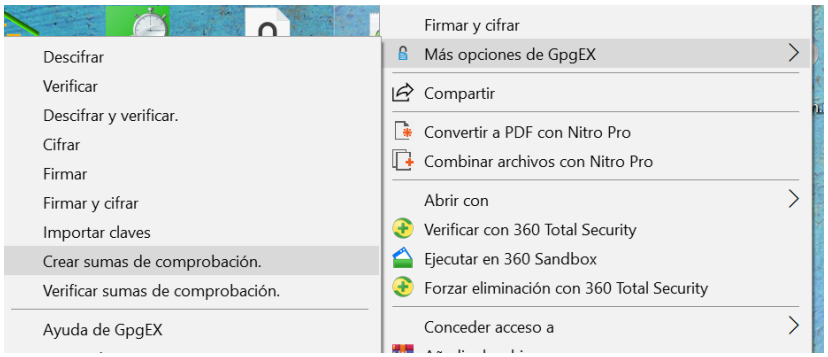
Verificaremos una firma asociada a un fichero y generada con Kleopatra. Necesitaremos el archivo de la firma .sig y el certificado generado anteriormente.

Para ello buscamos el .sig que contiene la firma y con el botón derecho del ratón pulsamos sobre “Descifrar verificar”.



9. Funciones de hash en Kleopatra

Podemos hacerlo seleccionando el fichero con el botón derecho del ratón “Crear sumas de comprobación”.



ENTREGA

Comprueba cada uno de los pasos de la operativa con Kleopatra. Para el último apartado puedes utilizar los ficheros de la práctica 2. Entrega captura de pantalla de la realización de cada uno de los 9 puntos.