

PROCEDIMENT DE L'ÚS DEL PROGRAMA D'ENCRIPCIÓ DE DADES GPG4WIN

Gpg4win és un paquet de xifrat de correu electrònic i arxius per a la majoria de les versions de Microsoft Windows, que utilitza criptografia de clau pública GnuPG per al xifrat de dades i signatures digitals.

La creació original de Gpg4win va ser secundat per l'Oficina Federal per a la Seguretat de la Informació d'Alemanya. No obstant això Gpg4win i totes les eines que s'inclouen són de programari lliure i de codi obert, i és en general l'opció no propietària de la vida privada recomanada per als usuaris de Windows.

Legislació

La Llei orgànica de Protecció de Dades de Caràcter Personal 03/2018 de 5 de desembre (LOPD), té per objecte protegir i garantir les llibertats i els drets fonamentals de les persones físiques, el seu honor i intimitat personal i familiar.

La LOPD estableix unes obligacions en relació a la protecció de dades de caràcter personal continguts en fitxers automatitzats i no automatitzats (en paper) que posseeixen empreses i administracions públiques, i que són tractats per aquestes amb diferents finalitats.

Després de l'anàlisi d'impacte dut a terme pel IBESTAT, en uns certs tractaments realitzats per aquest, s'ha identificat la necessitat d'implementar salvaguardes que protegeixin la informació gestionada d'aquelles amenaces que, després de la pertinent anàlisi de riscos, suposin un risc elevat per a les diferents dimensions de la seguretat. Entre aquestes salvaguardes i en relació amb la present instrucció, destaca la implementació de polítiques de xifratge de la informació a fi de garantir la confidencialitat d'aquesta.

La **criptografia asimètrica** (en anglès *asymmetric key cryptography*), també anomenada **criptografia de clau pública** (en anglès *public key cryptography*) o **criptografia de dues claus**¹ (en anglès *two-key cryptography*), és el mètode [criptogràfic](#) que usa un parell de claus per a l'enviament de missatges. Les dues claus pertanyen a la mateixa persona que rebrà el missatge. Una clau és pública i es pot lliurar a qualsevol persona, l'altra clau és privada i el propietari ha de guardar-la de manera que ningú tingui accés a ella. A més, els mètodes criptogràfics garanteixen que aquesta parella de claus només es pot generar una vegada, de manera que es pot assumir que no és possible que dues persones hagin obtingut casualment la mateixa parella de claus.

Si una persona que emet un missatge a un destinatari, usa la clau pública d'aquest últim per a xifrar-lo; una vegada xifrat, només la clau privada del destinatari podrà desxifrar el missatge, ja que és l'únic que hauria de conèixer-la. Per tant s'aconsegueix la *confidencialitat* de l'enviament del missatge, és *extremadament difícil que el desxifri algú excepte el destinatari*.


¹ https://ca.wikipedia.org/wiki/Criptografia_de_clau_p%C3%BAblica

Qualsevol, usant la clau pública del destinatari, pot xifrar-li missatges; els que seran desxifrats pel destinatari usant la seva clau privada.

Si el propietari del parell de claus usa la seva clau privada per a xifrar un missatge, qualsevol pot desxifrar-lo utilitzant la clau pública del primer. En aquest cas s'aconsegueix la *identificació i autenticació* del remitent, ja que se sap que només podia haver estat ell qui va emprar la seva clau privada (tret que un tercer l'hagi obtingut). Aquesta idea és el fonament de la [signatura digital](#), on jurídicament existeix la presumpció que el signant és efectivament l'amo de la clau privada.

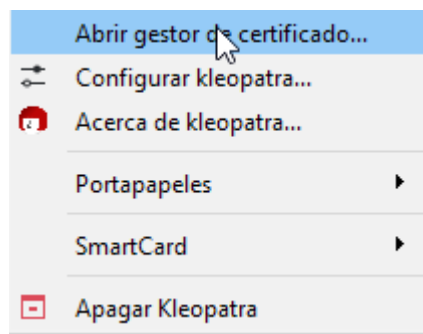
Els 'sistemes de xifratge de clau pública' o 'sistemes de xifratge asimètrics' es van inventar amb la finalitat d'evitar per complet el problema de l'intercanvi de claus dels [sistemes de xifratge simètrics](#). Amb les claus públiques no és necessari que el remitent i el destinatari es posin d'acord en la clau a emprar. Tot el que es requereix és que, abans d'iniciar la comunicació secreta, cadascun ha d'aconseguir la clau pública de l'altre i cuidar cadascun la seva clau privada. És més, aquestes mateixes claus públiques poden ser usada per qualsevol que desitgi comunicar-se amb algun d'ells sempre que s'utilitzi correctament la clau pública de cadascun.

Creació i enviament de clau pública en Gpg4win

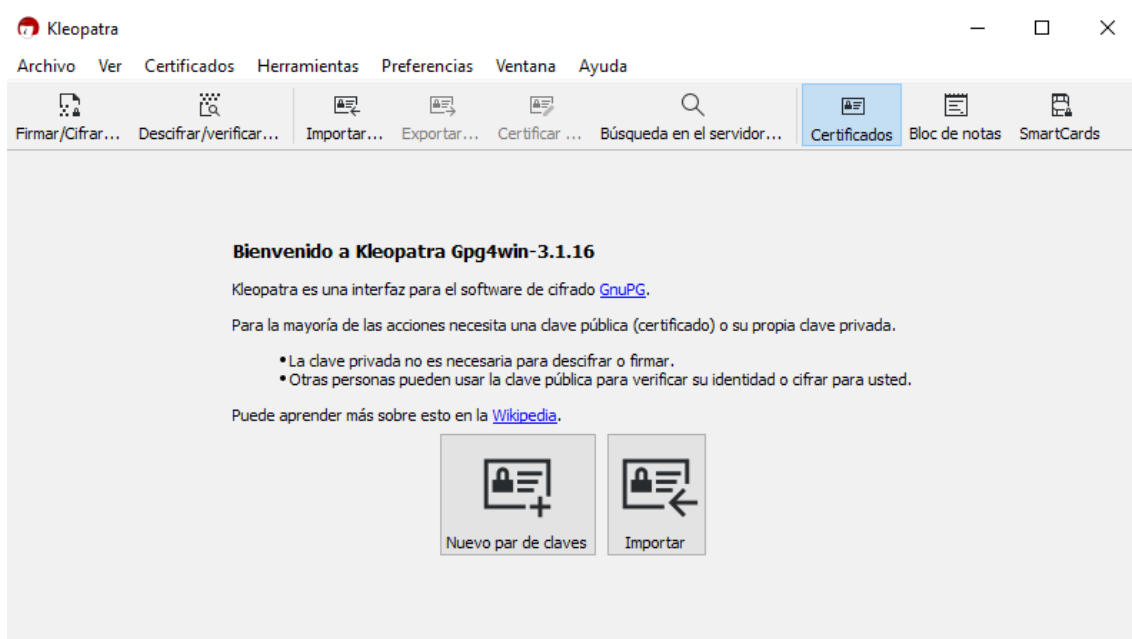
Una vegada instal·lat i reiniciat el sistema, podem anar a la barra de tasques de Windows (on es troba el rellotge del sistema) i li donem a la icona que simbolitza un cap vermell. 

Aquesta icona ens permet obrir l'eina Kleopatra per a la gestió dels certificats i per a encriptar/desencriptar els fitxers.

Li donem al botó dret sobre aquesta icona i ens mostra la finestra següent:



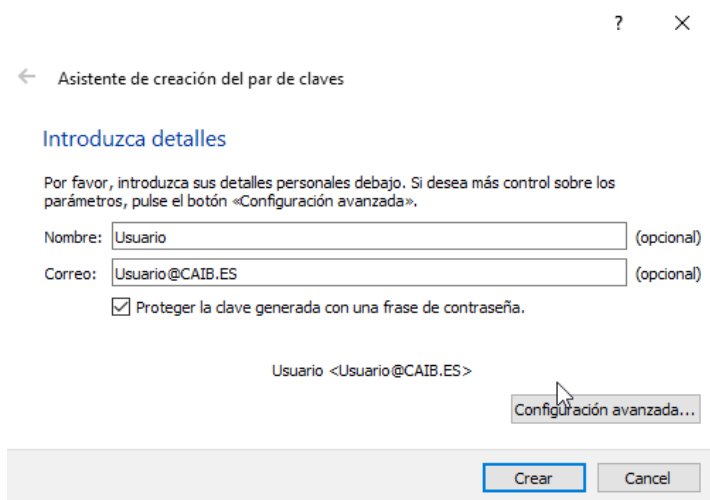
Seleccionem l'opció d'obrir el gestor de certificat.



En obrir el programa trobats dues principals opcions, la de generar un nou parell de claus (que ens permet generar la clau pública que podrem compartir i la clau privada que conté la contrasenya que ens permetrà desencriptar els fitxers que ens enviïn amb la pública).

l'opció d'Importar, que ens permet importar al nostre repositori les claus públiques d'altres persones/entitats, per a poder fer la tasca d'encriptar els fitxers que els hem d'enviar amb la seguretat necessària.

En seleccionar l'opció de generar un nou parell de claus, s'obrirà un assistent per a poder crear la nostra clau pública que utilitzarem per a encriptar fitxers que vagin destinats a nosaltres, ens demanarà el nom que volem que surti, la nostra adreça de correu electrònic i després li podrem assignar una clau privada que només coneixerem nosaltres en principi i ens servirà per a obrir i descriptar el fitxer que ens enviïn.



Asistente de creación del par de claves

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)

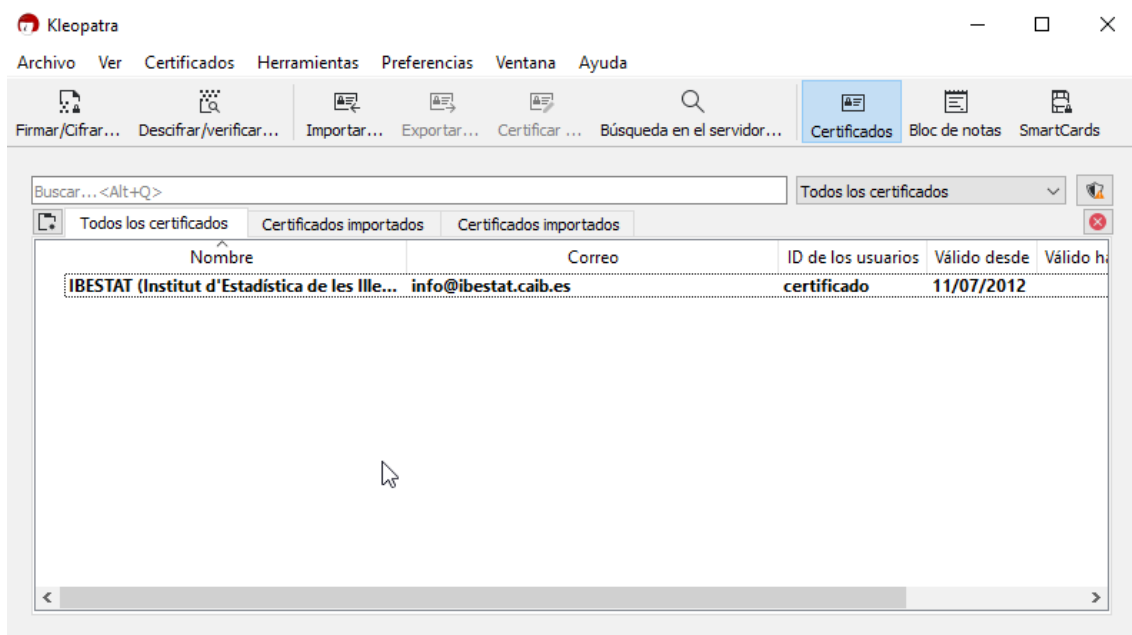
Proteger la clave generada con una frase de contraseña.

Usuario <Usuario@CAIB.ES>

Configuración avanzada...

Crear Cancel

Una vegada creada la clau pública que compartirem sortirà en el llistat de "Certificats", el millor és exportar la clau pública i enviar-la a qui ens encriptarà dades ja que en realitzar el procés indiqués que el faci amb les nostres dades i només nosaltres podrem visualitzar el contingut amb la nostra clau.



Kleopatra

Archivo Ver Certificados Herramientas Preferencias Ventana Ayuda

Firmar/Cifrar... Descifrar/verificar... Importar... Exportar... Certificar... Búsqueda en el servidor... Certificados Bloc de notas SmartCards

Buscar...<Alt+Q> Todos los certificados

Nombre	Correo	ID de los usuarios	Válido desde	Válido hasta
IBESTAT (Institut d'Estadística de les Ille...	info@ibestat.caib.es	certificado	11/07/2012	

Ens col·loquem damunt de la clau que volem exportar i amb el botó dret li donem a exportar, ens creés un fitxer amb extensió “ASC”, i és el que hem d'enviar perquè ens puguin encriptar amb la nostra clau, si aquesta persona rep aquesta clau pública nostra, l'importés en el seu joc de claus i quan hagi d'encriptar alguna cosa per a nosaltres ho farà amb aquesta clau pública.

Desencriptar fitxers encriptats

Per a desencriptar només cal anar al fitxer en concret, i li donem al botó dret, després a l'opció de:

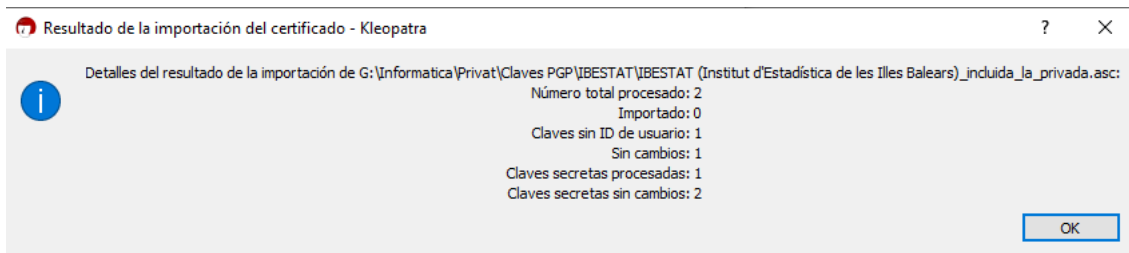


llavors ens demanarà la clau privada associada a aquest fitxer que serà la que vam posar al principi en crear el parell de claus.

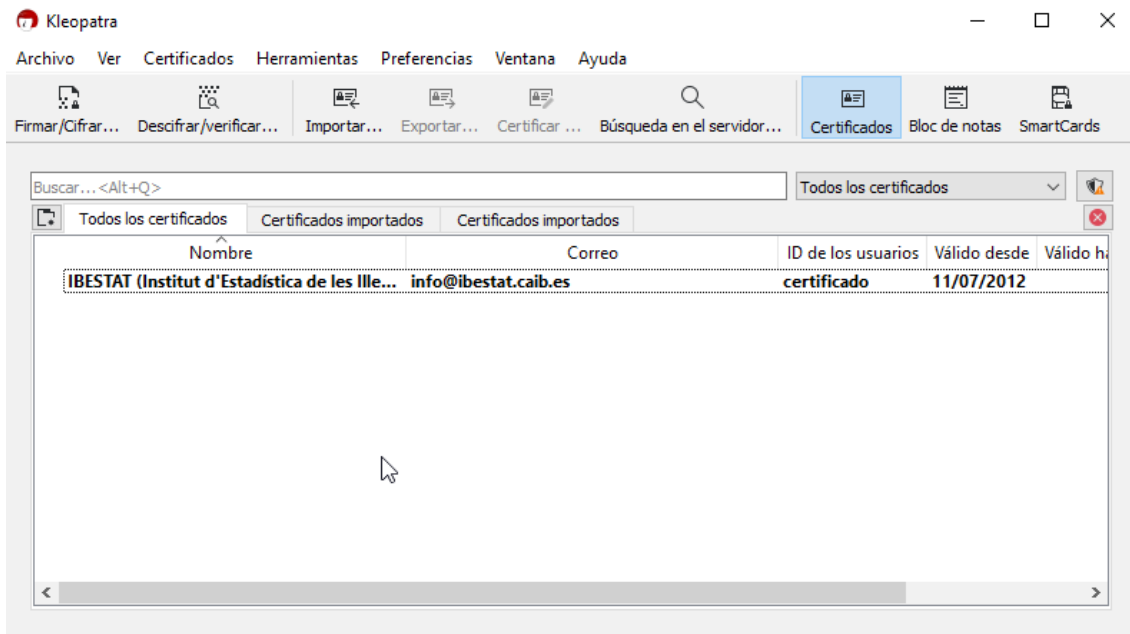
Encriptar dades amb claus públiques

Per a poder enviar fitxers encriptats a algú, hem de disposar de la seva clau pública perquè només ell pugui desencriptar el contingut amb la clau privada associada.

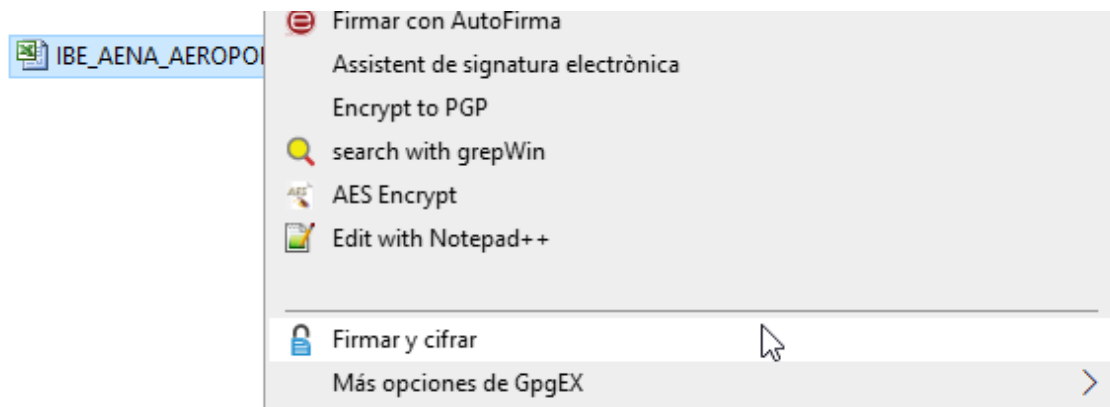
Per a importar la clau pública d'algú procedirem a donar-li doble clic al fitxer que ens envien amb extensió “ASC” i tot seguit ens mostra automàticament la següent finestra:

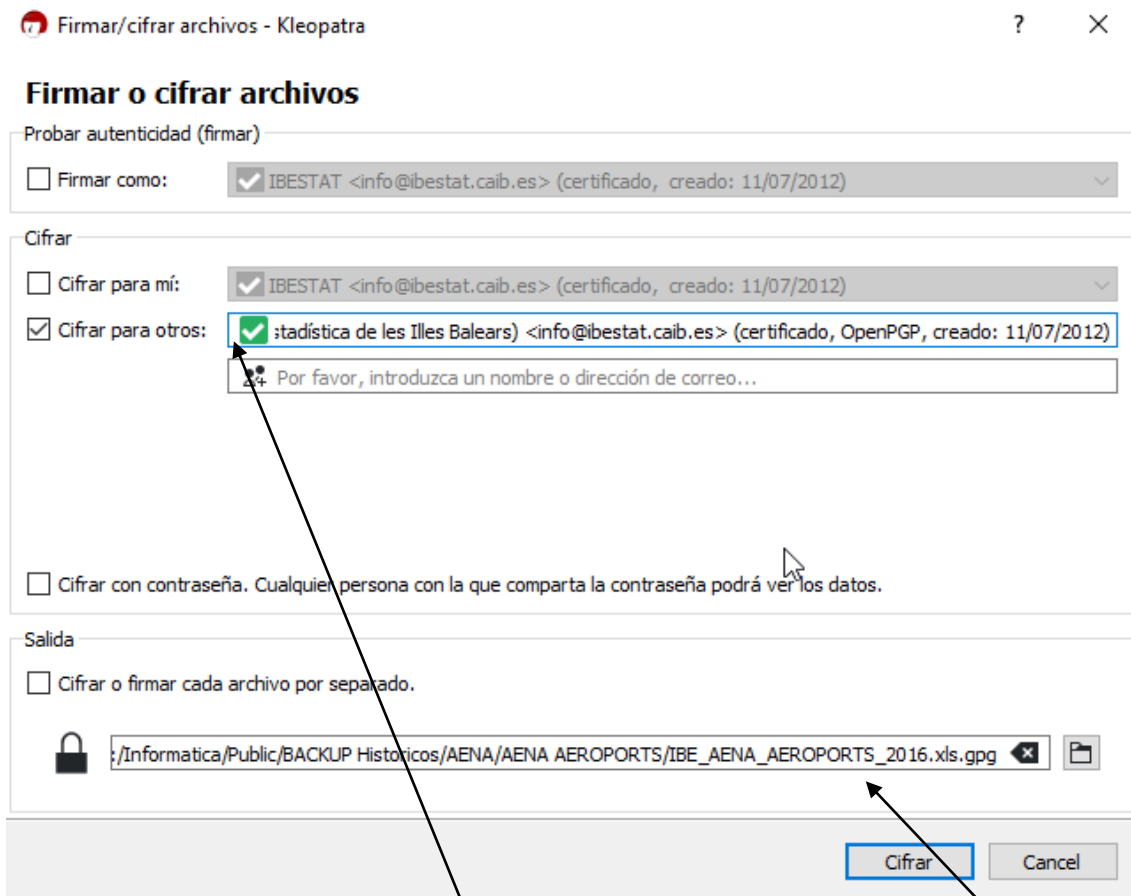


En obrir la interface de Kleopatra, ens apareix ja el certificat (clau pública), que hem importat i ja podem utilitzar-la per a encriptar els fitxers a enviar i que només el destinatari amb la seva clau privada podrà desencriptar.



El procés per a encriptar és més senzill, simplement ens col·loquem damunt del fitxer a encriptar i premem el botó dret, en aparèixer el menú contextual seleccionarem

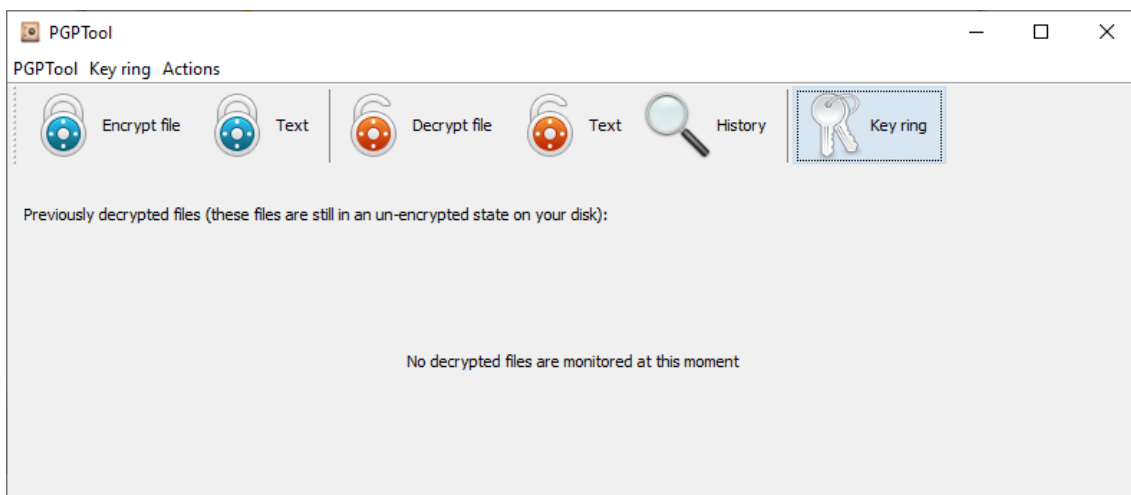




Hem d'indicar la clau publica del destinatari, i posteriorment indicar-li el directori de sortida on se situés el fitxer encriptat.

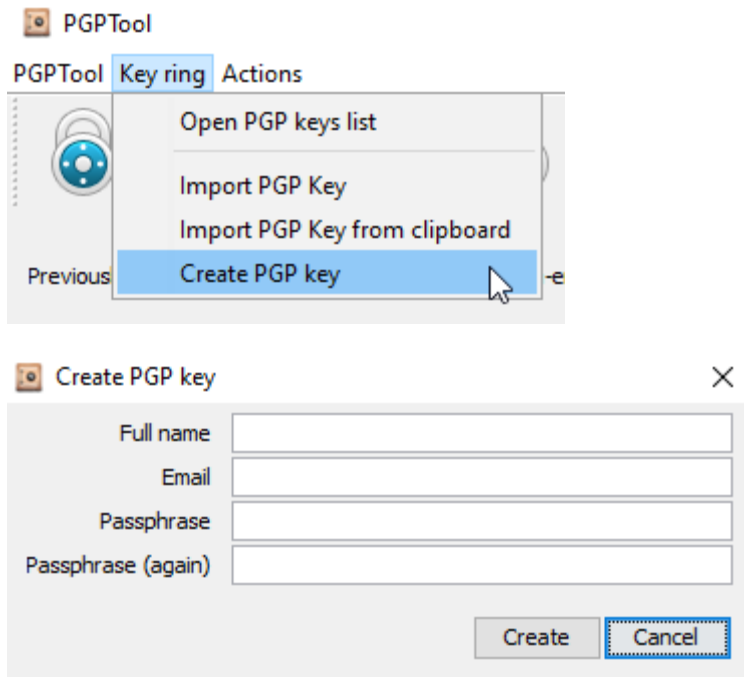
PGPtool

Existeix una alternativa al programa Gpg4win, i és una eina anomenada PGPtool, el seu funcionament és molt similar a l'anterior, però és més lleuger i senzill d'utilitzar.



Aquest programa requereix tenir instal·lat en el sistema el JAVA RUNTIME ENVIRONMENT +18, per a funcionar.

Per a crear des d'aquest programa la clau pública i privada, es realitza a través del corresponent menú:



La pàgina per a la seva descàrrega i instruccions d'ús es troba disponible en:

<https://pgptool.github.io>