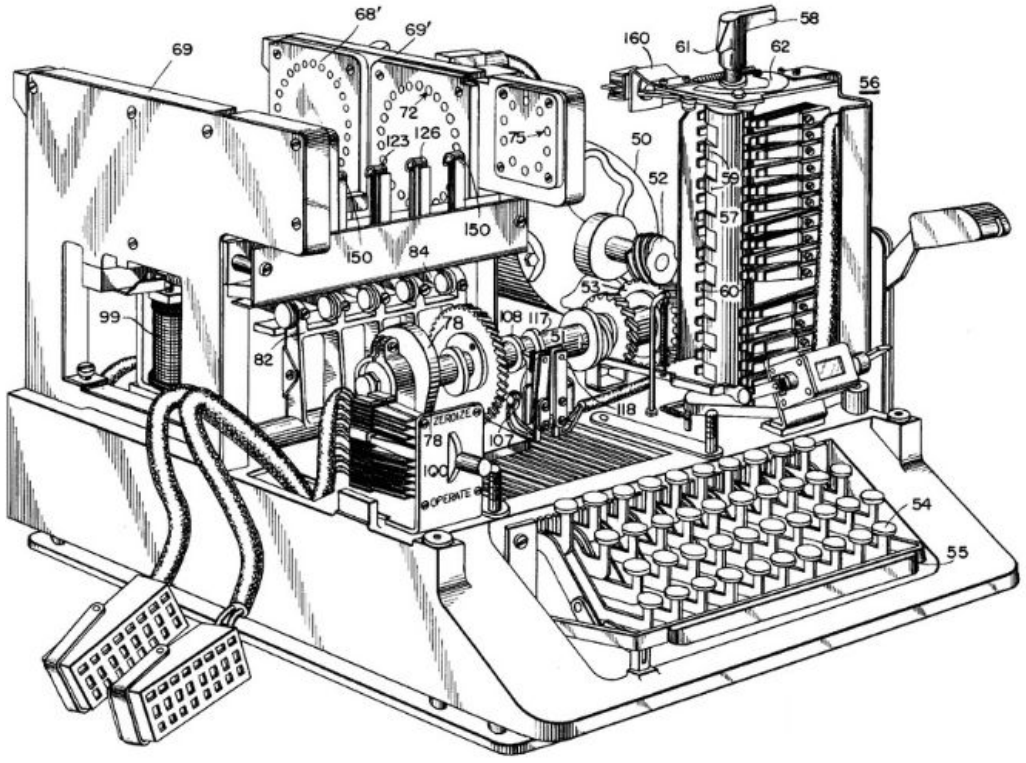
BLOCKCHAIN ESPAÑA

Guía de instalación
GnuPG + Thunderbird + Enigmail (Windows)



Javier Domínguez Gómez

v0.03 - 2017

Introducción

Este documento es una guía de instalación y configuración de **GnuPG**, software libre de cifrado para comunicaciones entre personas en un medio digital como pueden ser una computadora o dispositivos móviles. También se detalla la instalación y configuración del cliente de correo **Thunderbird** y el complemento **Enigmail**, que integra GnuPG con el cliente de correo. He creado este documento para complementar los futuros eventos relacionados con criptografía, privacidad y derechos del usuario en la red que organiza periódicamente de **Blockchain España** como movimiento social.

El objetivo principal de esta guía es ayudar al usuario a instalar estos tres componentes, necesarios para poder generar o crear un par de claves (pública y privada) y aplicar las buenas prácticas para mantener comunicaciones más seguras y encriptadas entre personas. Una vez realizado este tutorial el usuario podrá ponerse en contacto con Blockchain España para gestionar correctamente el intercambio de claves públicas.

Puedes imprimir, copiar o distribuir este documento libremente, siempre que se mencione la fuente original. Cualquier duda, consulta, error o corrección a la hora de seguir esta guía puedes contactar con Blockchain España en el correo blockchainespana@gmail.com, en el grupo oficial de Telegram o en Twitter (@BlockchainES). También se puede contactar directamente conmigo en el correo jdg@member.fsf.org, en Telegram o en Twitter.

Mi clave pública es: 0x5BDCC668D6648E2B

Enlaces de Interés

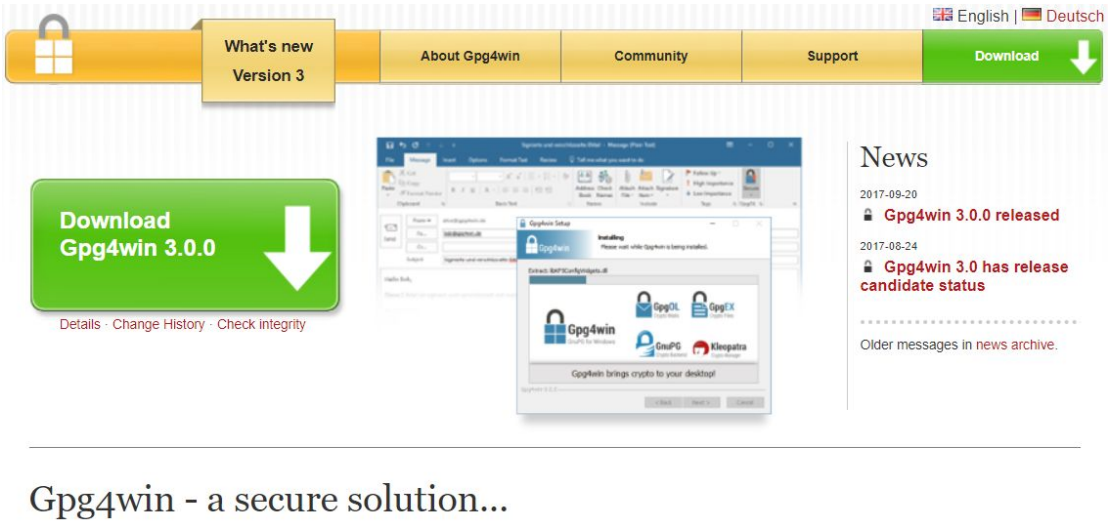
- Grupo Telegram “Blockchain España Key signing party”: https://t.me/KeyParty
- Grupo Telegram “Blockchain España Comunidad”: https://t.me/blockchainespana
- GnuPG (Wikipedia): https://es.wikipedia.org/wiki/GNU_Privacy_Guard
- Thunderbird (Wikipedia): https://es.wikipedia.org/wiki/Mozilla_Thunderbird
- Enigmail (Wikipedia): https://es.wikipedia.org/wiki/Enigmail
- Biglumber: http://www.biglumber.com

Este obra está bajo una licencia de:
Creative Commons Reconocimiento-NoComercial 4.0 Internacional.

1. El primer paso es descargar GnuPG para Windows. Para ello hay que entrar en la siguiente dirección web:

   https://www.gpg4win.org

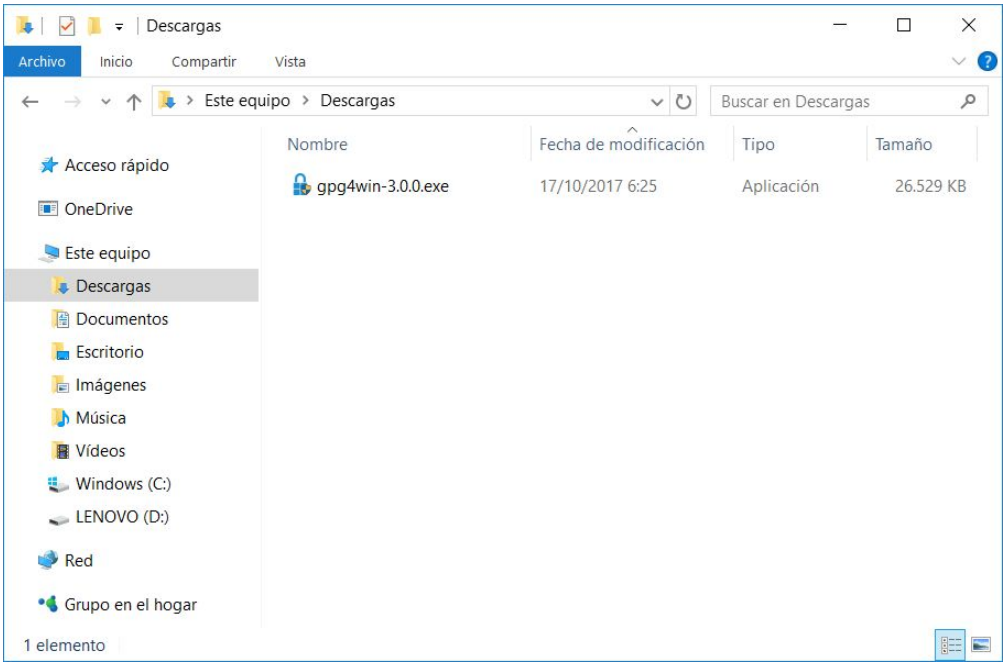
2. Hacer click en el botón "**Download Gpg4win 3.0.0**"



3. Seleccionar la opción que se considere oportuna, si no se quiere donar nada y descargar Gpg4win gratis solo hay que pulsar sobre el botón que pone "**$0**" y a continuación en el botón "**Download**".

4. Aparecerá la siguiente pantalla y comenzará la descarga:

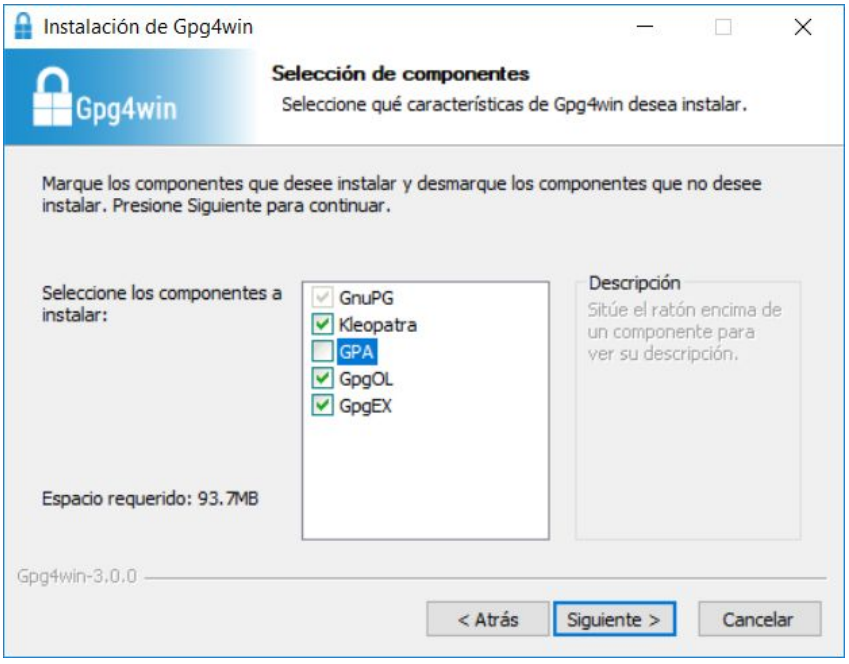
5. En la carpeta "**Descargas**" se puede encontrar el archivo ejecutable descargado, se llama **gpg4win-3.0.0.exe**. Para ejecutarlo hay que pulsar doble click sobre él.



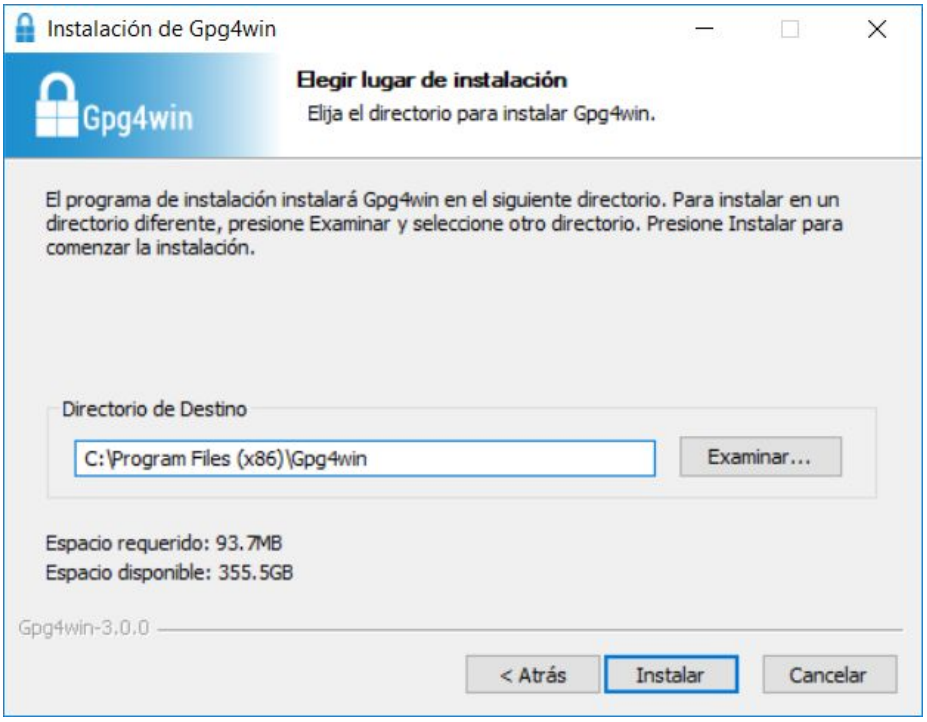
6. Seleccionar el idioma preferido, para este manual se ha elegido "**Español**".

7. En la primera pantalla solo hay que pulsar el botón “**Siguiente**”:

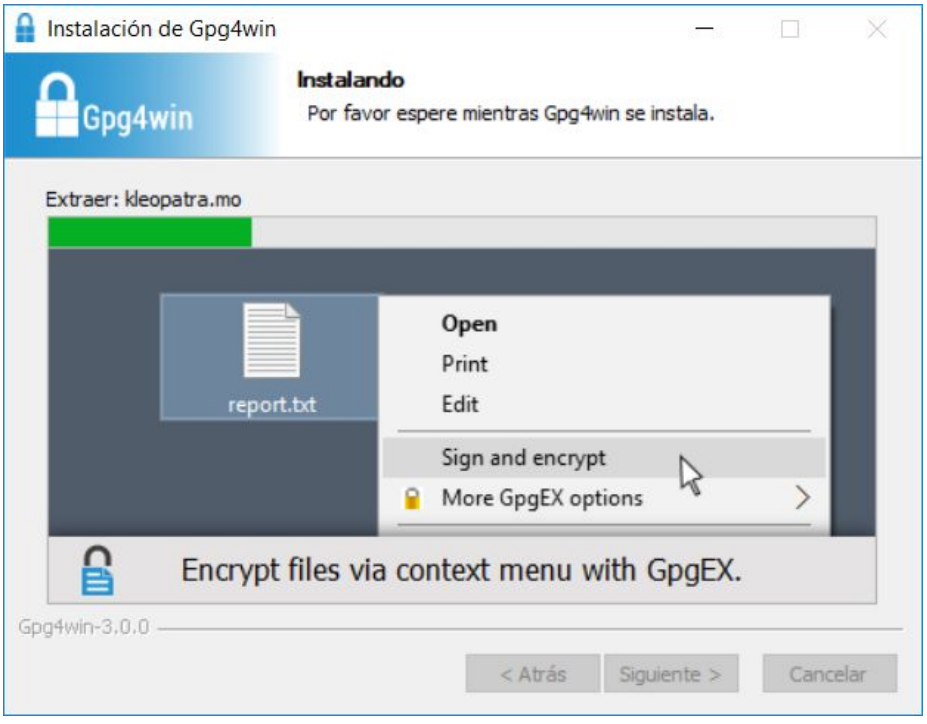
8. Sin modificar nada se pulsa de nuevo el botón “**Siguiente**”:



9. Se puede cambiar la ruta de instalación si se desea, si no se deja la que viene por defecto. Se pulsa el botón "**Instalar**":



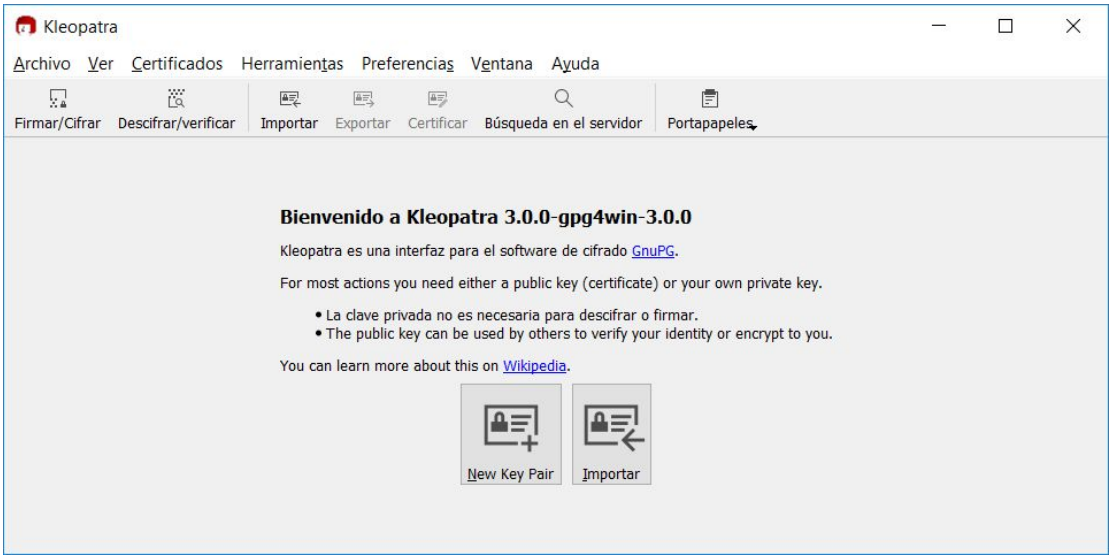
10. Comienza la instalación:



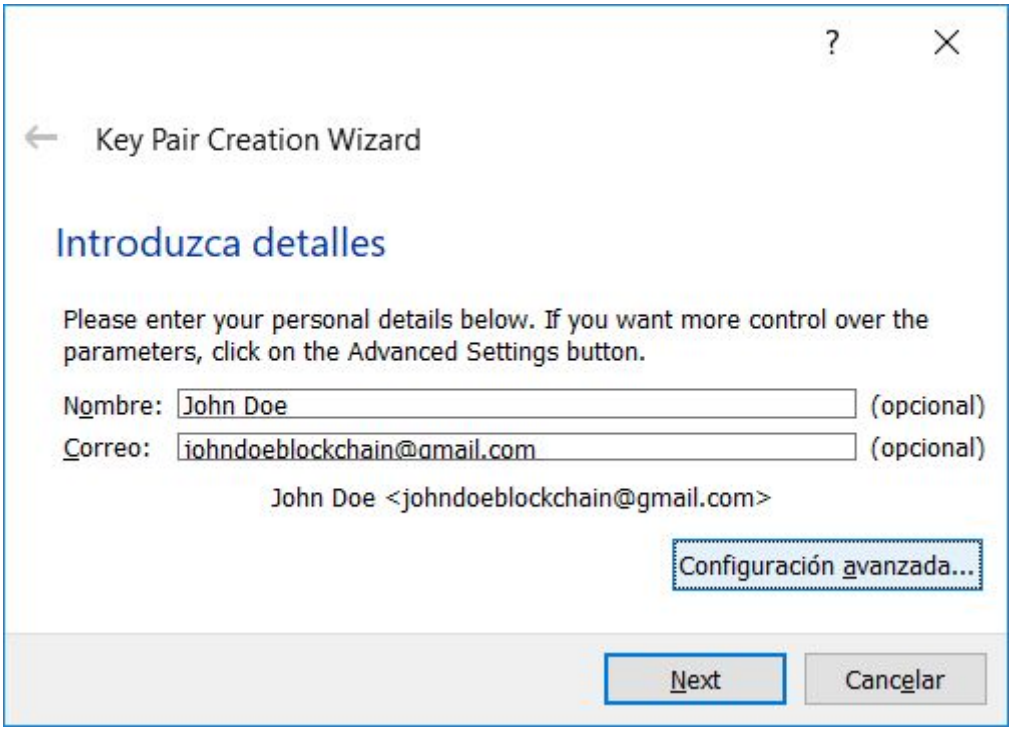
11. Cuando finalice la instalación pulsar el botón “**Siguiente**”:

12. Finalmente pulsar el botón “**Terminar**”:

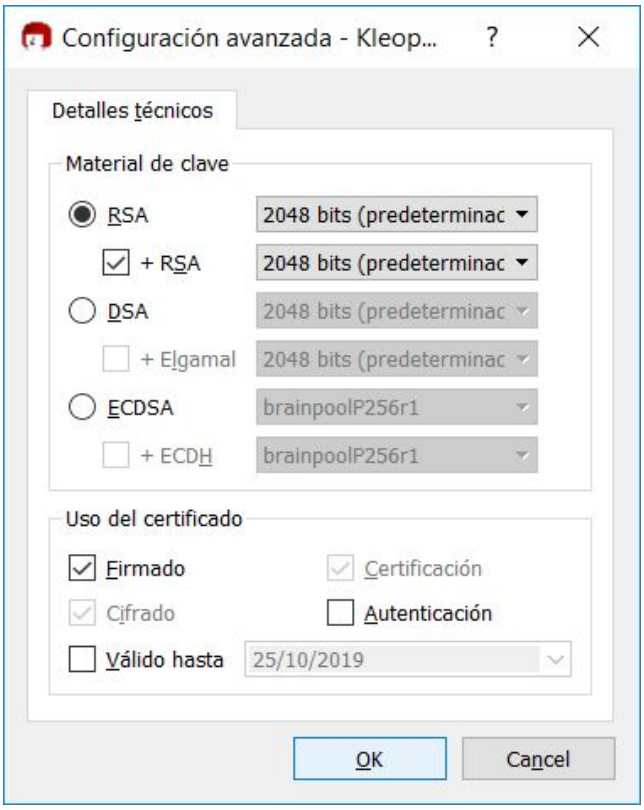
13. Se abrirá el programa Kleopatra. Pulsar sobre el botón central “**New Key Pair**”:



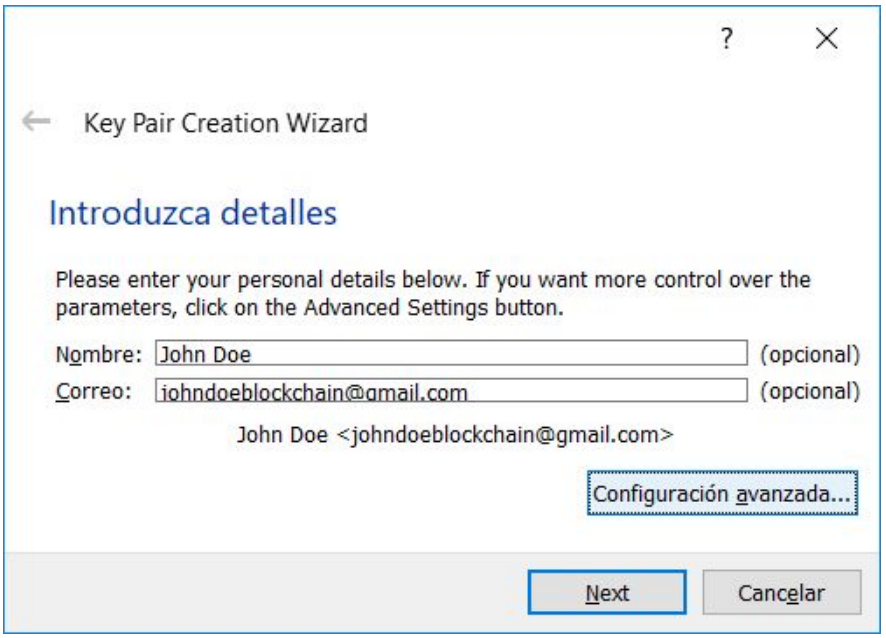
14. En el campo opcional “**Nombre**” hay que poner el nombre con el que se quiere asociar el par de claves (*pública/privada*), en este ejemplo se ha puesto el nombre **John** y el apellido **Doe**, y en el campo opcional “Correo” se ha de añadir la dirección mail también asociado al par de claves, en este ejemplo se ha puesto **johndoeblockchain@gmail.com**. Antes de pulsar en el botón “**Next**” se puede pulsar en el botón “**Configuración avanzada…**” para ver las diferentes opciones de cifrado:



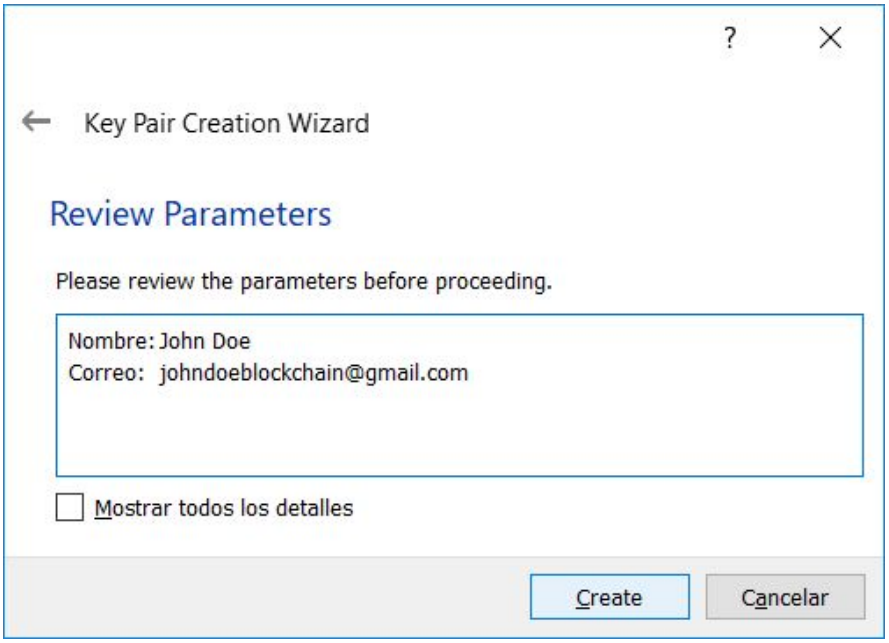
15. Si no hay una preferencia concreta para cambiar de algoritmo de encriptación de deja como aparece en la imagen de ejemplo, todo por defecto, y se pulsa el botón "**OK**", pero si se desea se puede seleccionar opciones alternativas de cifrado. Ojo: El algoritmo de curva elíptica (*ECDSA*) no es compatible con todos los servidores de claves (todavía):



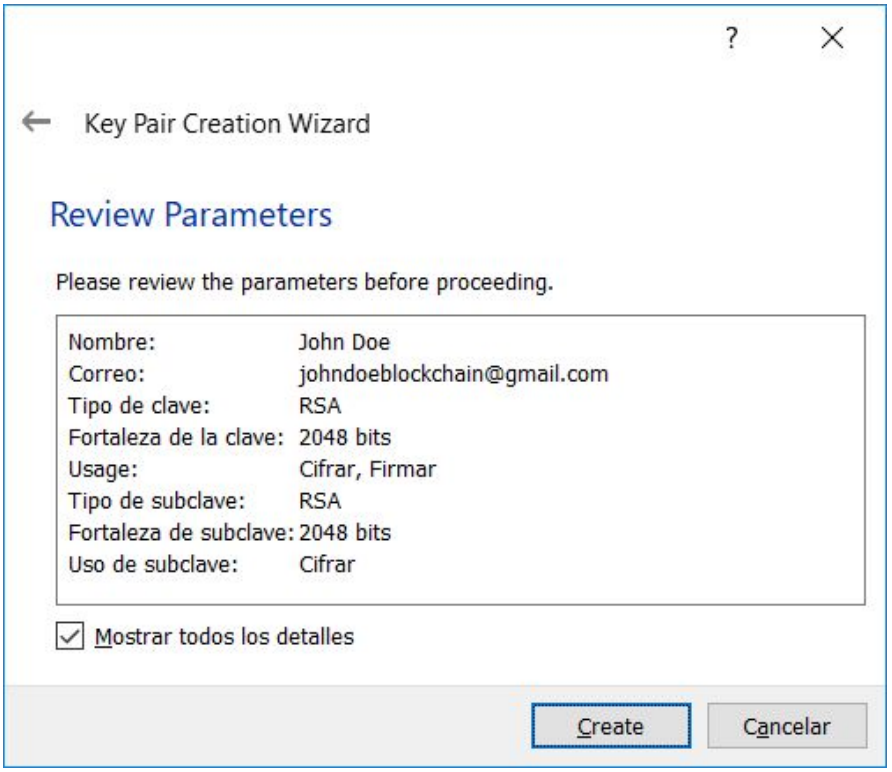
16. Aparecerá la ventana de antes, ahora se puede pulsar el botón "**Next**":



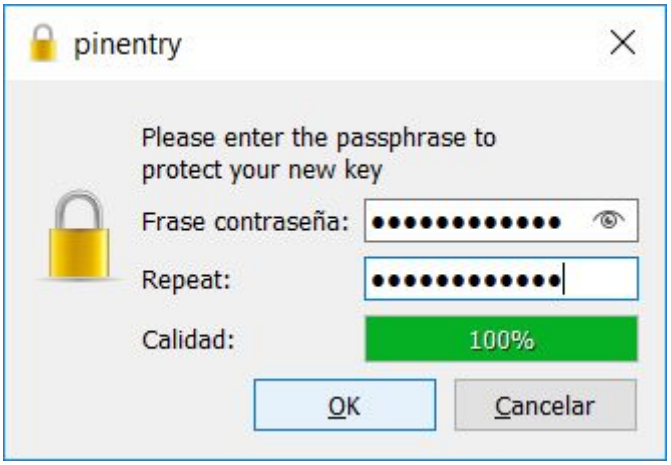
17. Si se desea se puede activar el checkbox que pone “**Mostrar todos los detalles**”.



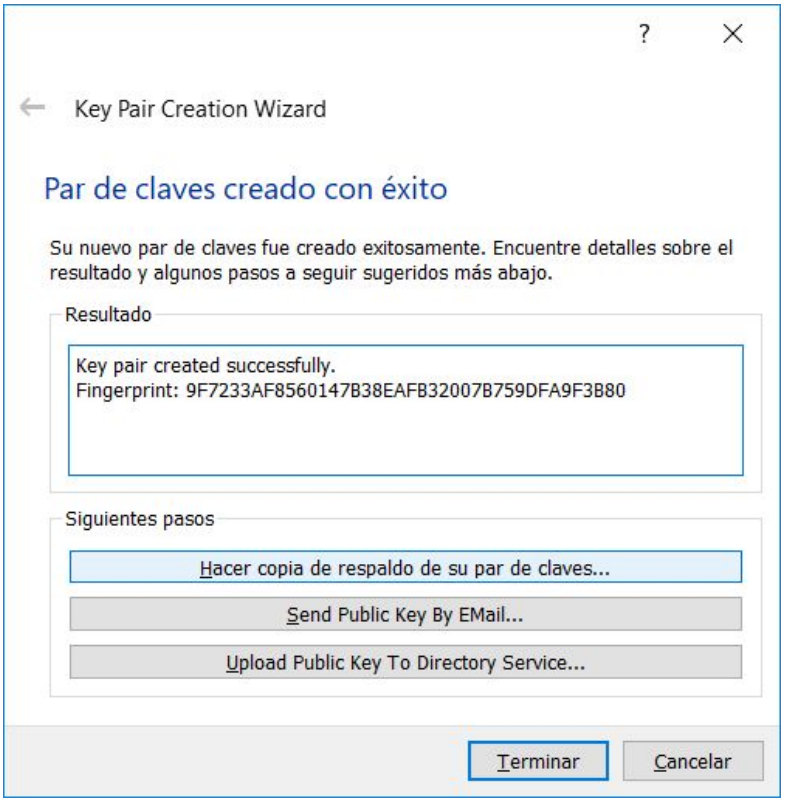
18. Se se ha activó la opción de “**Mostrar todos los detalles**” en el paso anterior aparecerá una pantalla como la siguiente en la que se puede ver un resumen con toda la configuración. Se pulsa el botón “**Create**”:



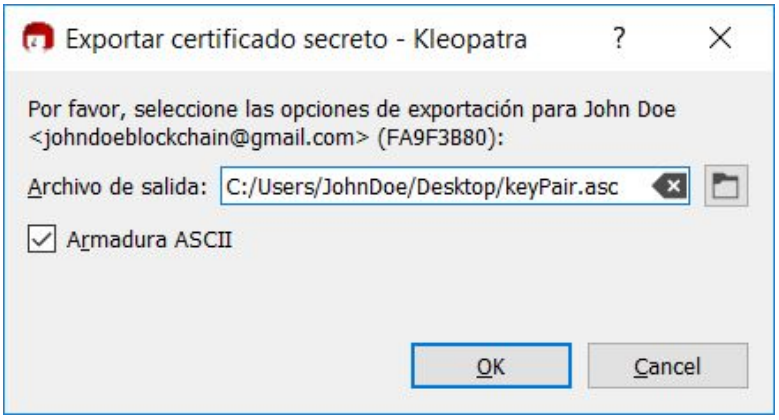
19. Aparecerá una ventana en la que se pide introducir la contraseña o *passphrase* que se pedirá cada vez que se utilice el par de claves para descifrar archivos o mensajes. Es **IMPORTANTÍSIMO** no perder esta clave, de lo contrario no se podrán volver a descifrar los mensajes o archivos cifrados. Pon una clave que no sea sencilla pero que al mismo tiempo sea fácil de recordar. Una vez introducida la clave pulsa OK:



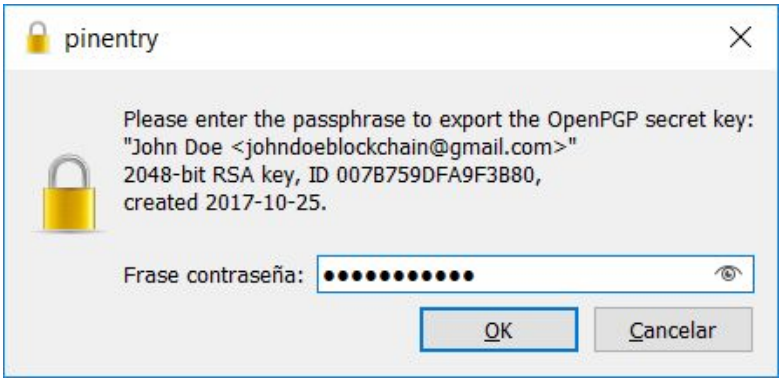
20. En este punto ya se han creado el par de claves. ahora aparece una ventana como la siguiente. Pulsar el botón que dice "**Hacer copia de respaldo de su par de claves...**" para exportar a un archivo las dos claves, o sea, la clave privada y la clave pública:



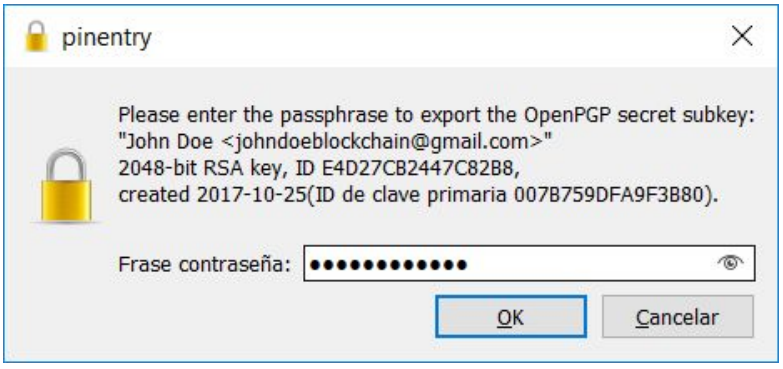
21. Hay que seleccionar una carpeta de destino para este archivo de respaldo y darle un nombre, en este ejemplo se le ha llamado **keyPair.asc**, pero se puede escoger el nombre que se quiera. Se ha de marcar el checkbox "**Armadura ASCII**" y después pulsar el botón "**OK**".



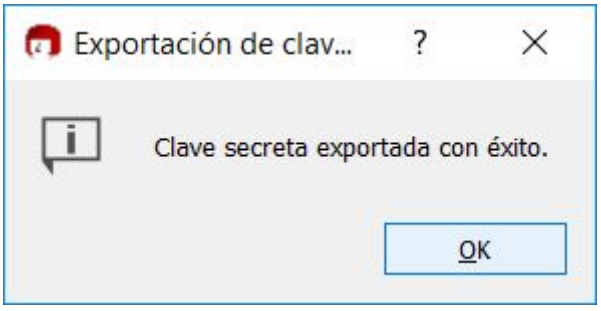
22. En esta nueva ventana se ha de introducir la password que se ha introducido anteriormente en el paso 19. Se pulsa el botón "**OK**":



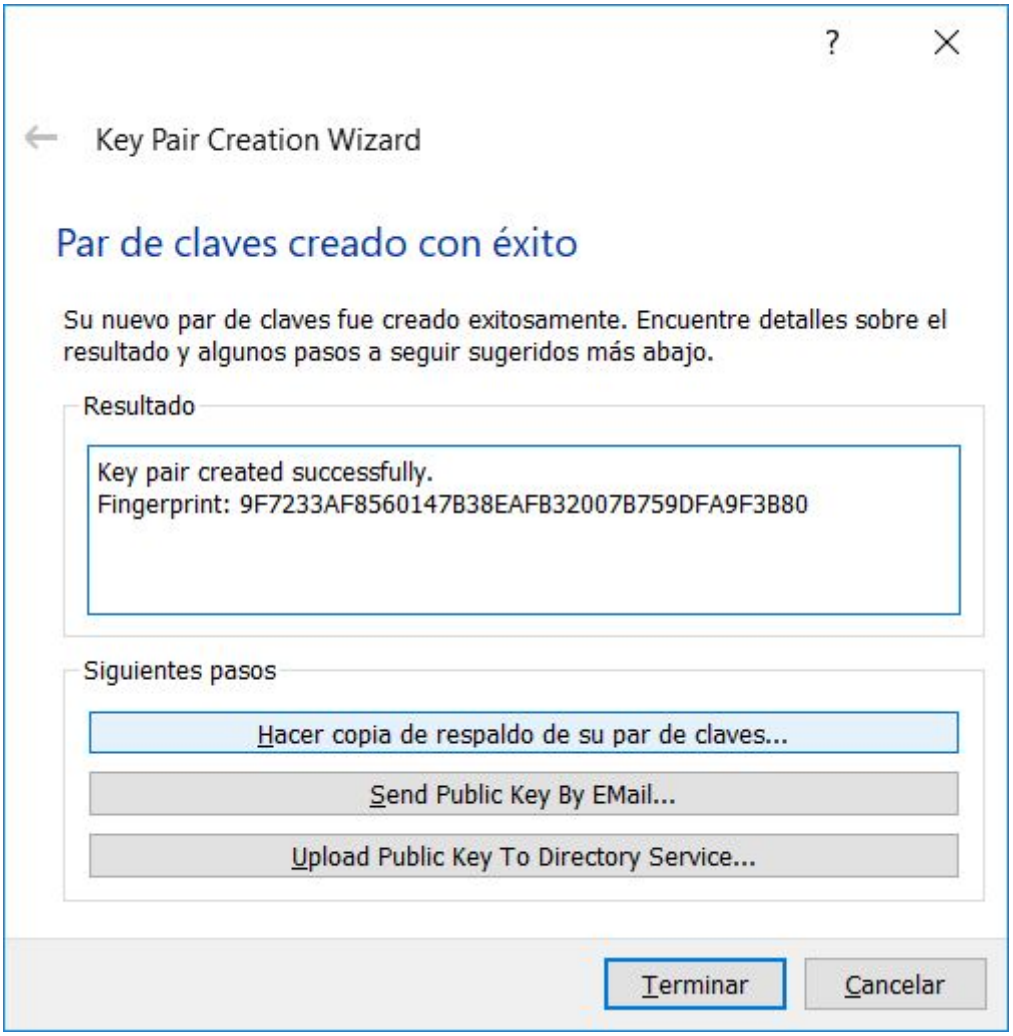
23. Y en esta otra venta se ha de introducir una vez más la misma password. Se pulsa el botón "**OK**":



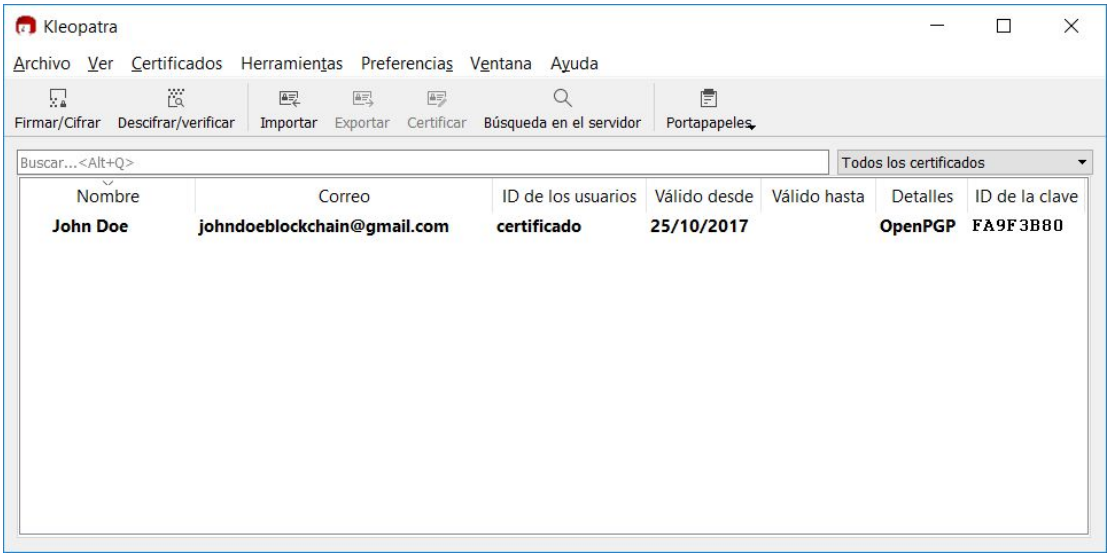
24. Aparece una ventana como la siguiente en la que confirma que todo ha salido correctamente:



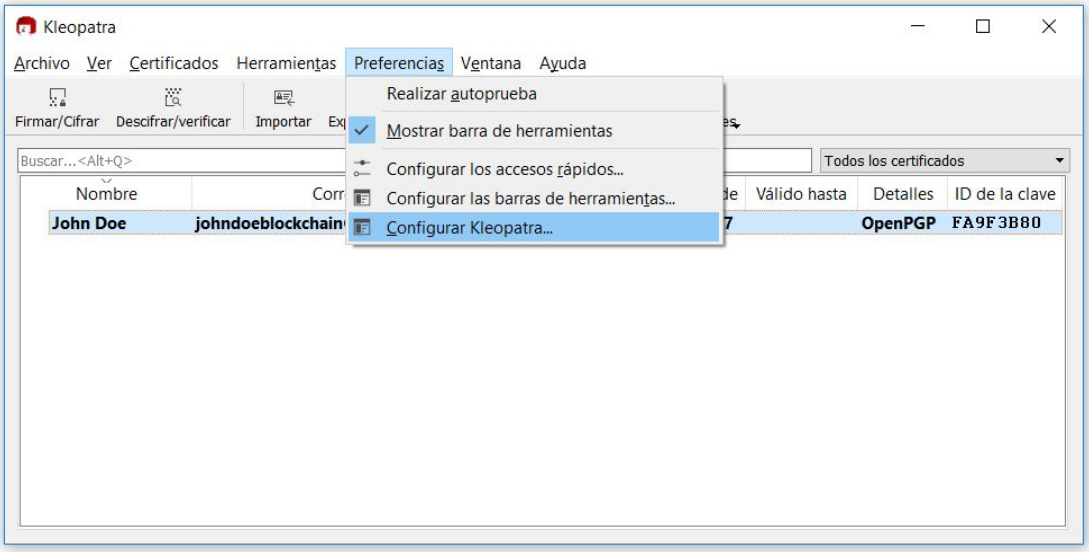
25. Se pulsa el botón "**Terminar**":



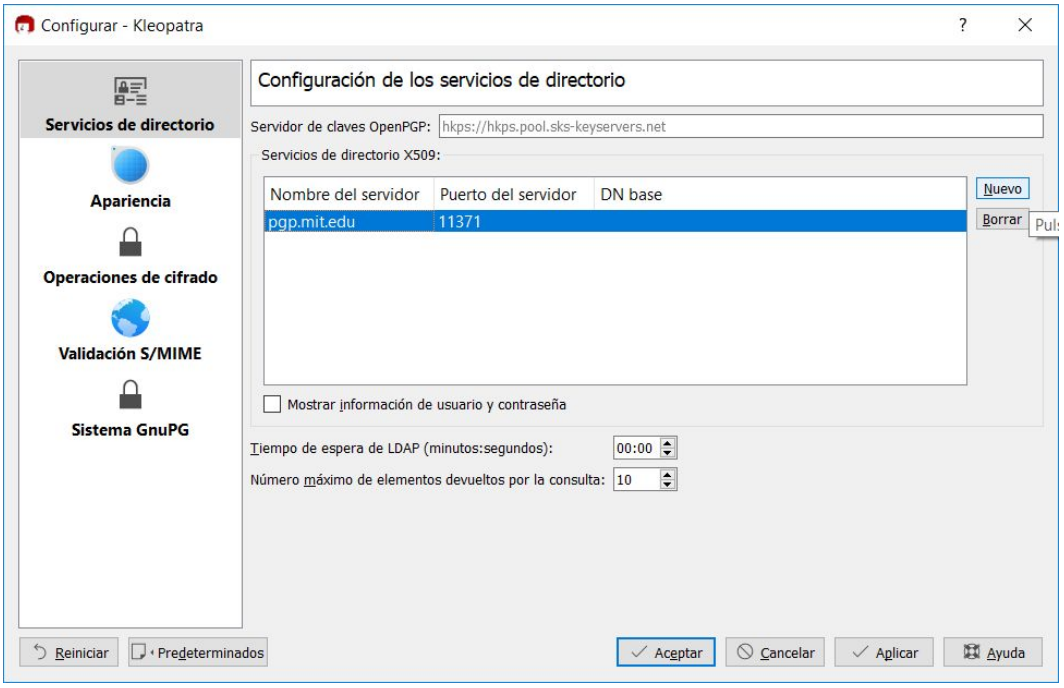
26. Esta es la ventana de **Kleopatra**, el programa que va a gestionar en este ordenador las claves públicas y privadas, tanto las propias como las de otras personas:



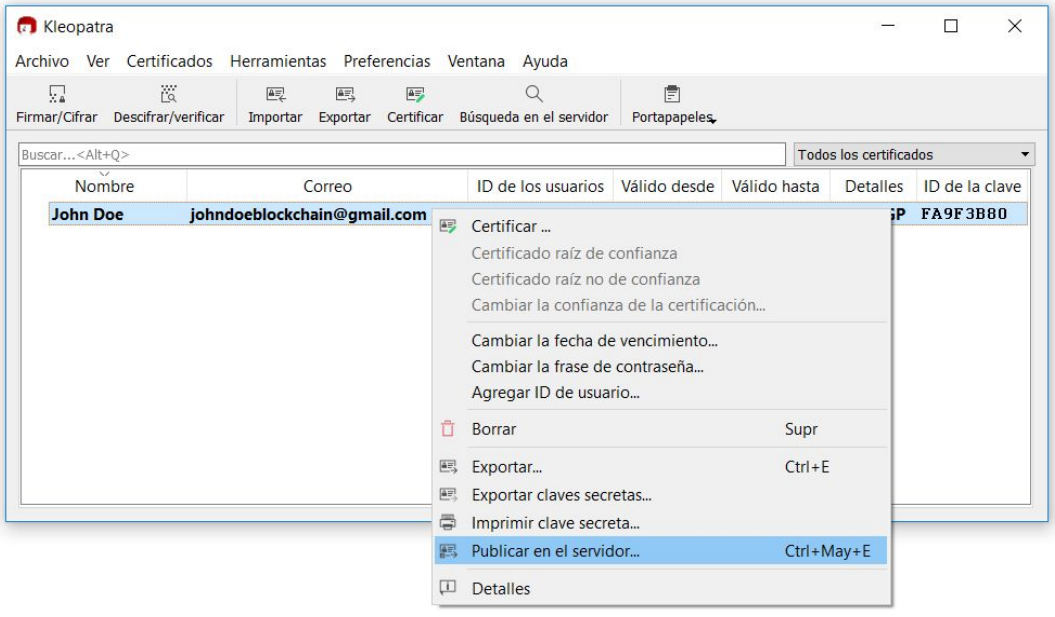
27. Hay que configurar algún servidor de claves al que luego poder subir o añadir la clave pública que se acaba de generar. Para ello hay que hacer click en "**Preferencias**" y luego en "**Configurar Kleopatra**":



28. Hay que añadir un servidor de claves. Para ello se pulsa en el botón “**Nuevo**” y se añade el nombre y el puerto. En este ejemplo se ha usado el servidor “**pgp.mit.edu**” y el puerto “**11371**”. Se pueden añadir todos los que se quiera, pero se ha de buscar previamente información sobre el nombre y el puerto. Para seguir este tutorial bastaría con el del ejemplo. Una vez añadido un servidor se pulsa primero el botón “**Aplicar**” y después el botón “**Aceptar**”:

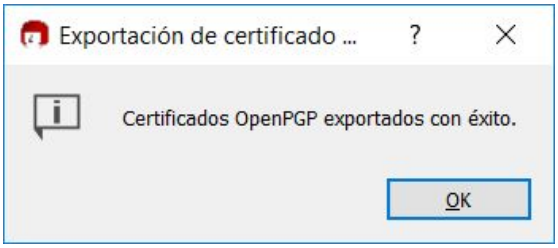


29. Para subir la clave pública a los servidores que se tengan configurados se ha de hacer click con el botón derecho sobre el nombre del certificado que aparece en Kleopatra, y seleccionar la opción “**Publicar en el servidor…**”:

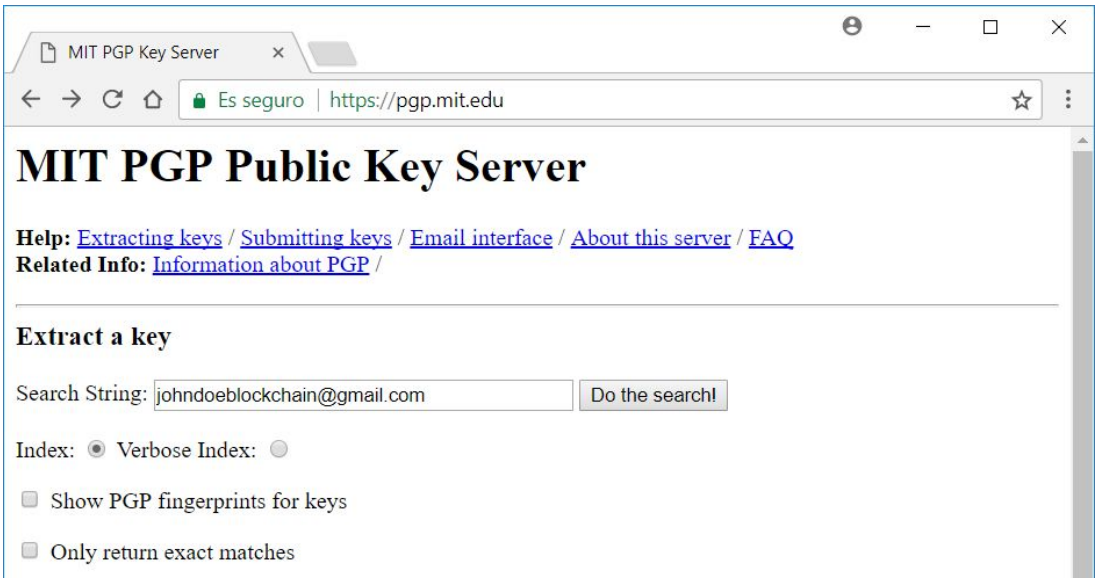


30. Aparecerá esta ventana pidiendo confirmación sobre querer subir el certificado a un servidor de claves. Se pulsa el botón “**Continuar**”:

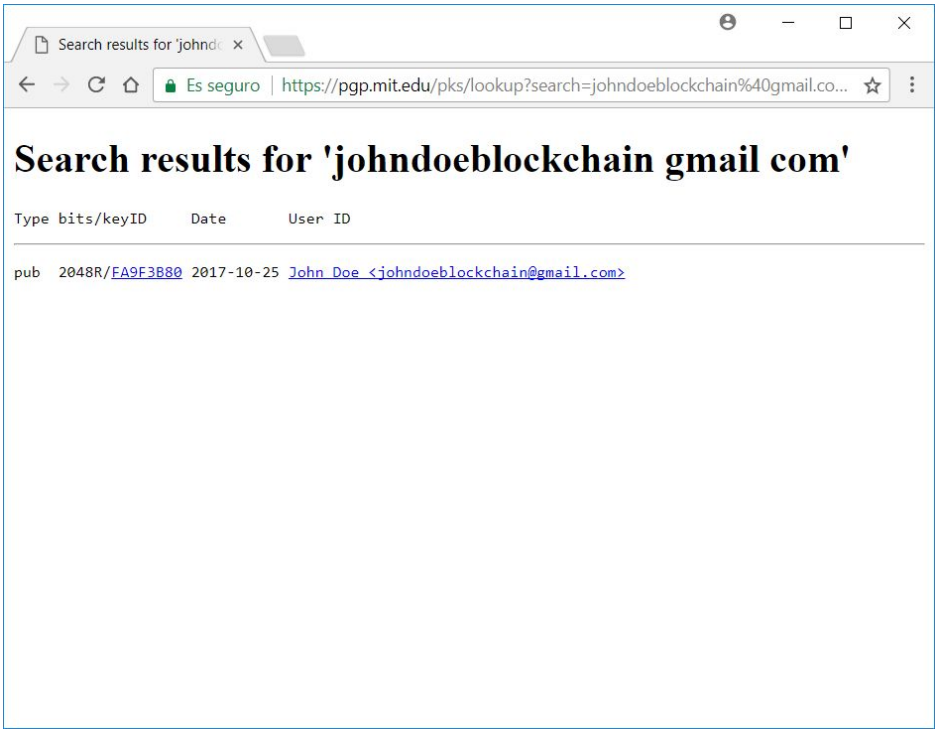
31. Aparece un mensaje indicando que el certificado se ha subido correctamente los servidores de claves que se tuvieran configurados. Se pulsa el botón “**OK**”:



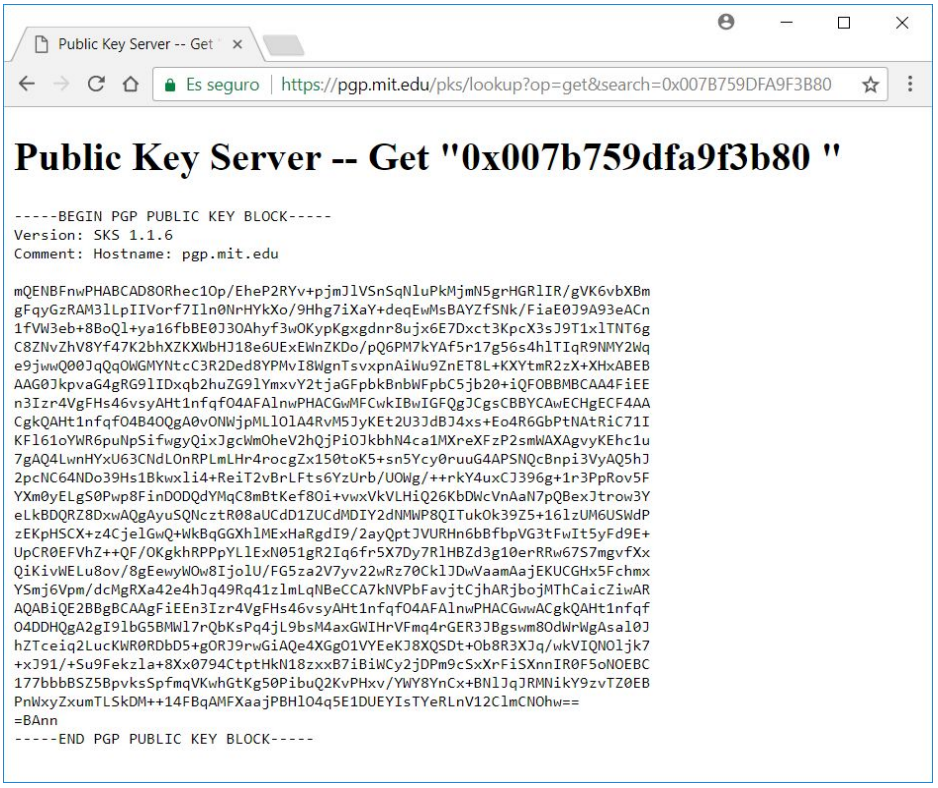
32. Finalmente hay que acceder a cualquiera de los servidores, en el caso de este ejemplo a la URL: https://pgp.mit.edu y buscar la clave pública, por ejemplo introduciendo el email que se escogió a la hora de crear el par de claves:



33. Si todo ha salido correctamente aparecerá el certificado que se ha subido desde Kleopatra.



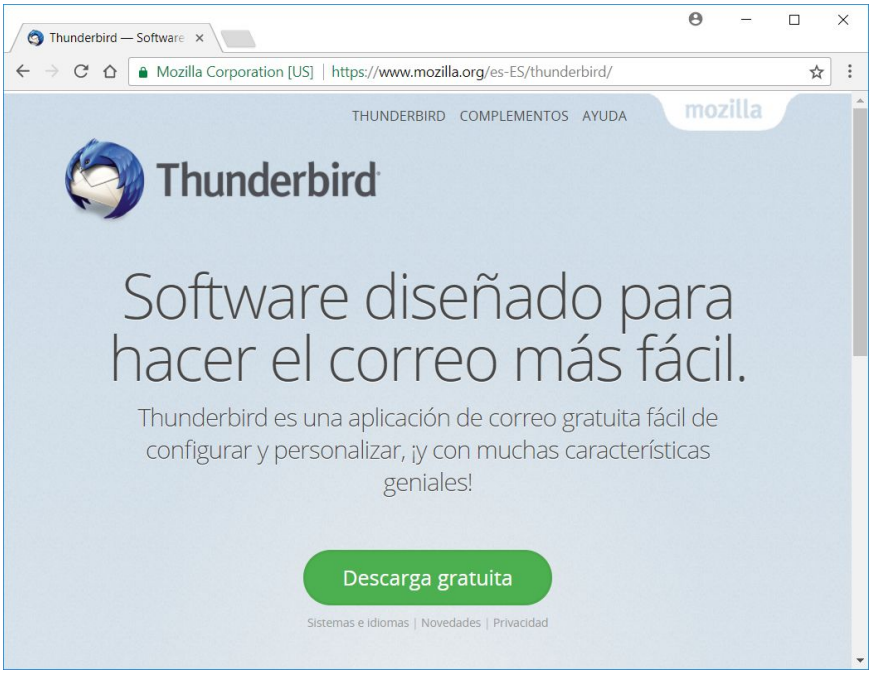
34. Al pinchar en el **keyID** se accede a una página donde aparece el texto que forma la clave pública:



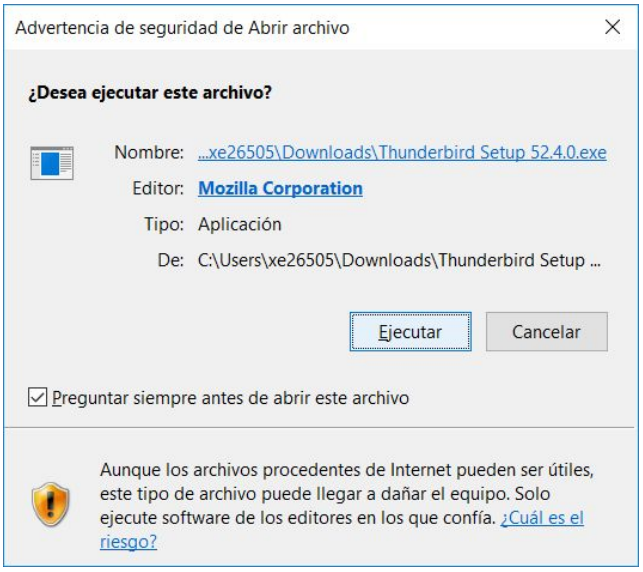
35. En este punto del documento se explica cómo descargar, instalar y configurar el cliente de correo Thunderbird. Hay que ir a la siguiente URL:

    https://www.mozilla.org/es-ES/thunderbird

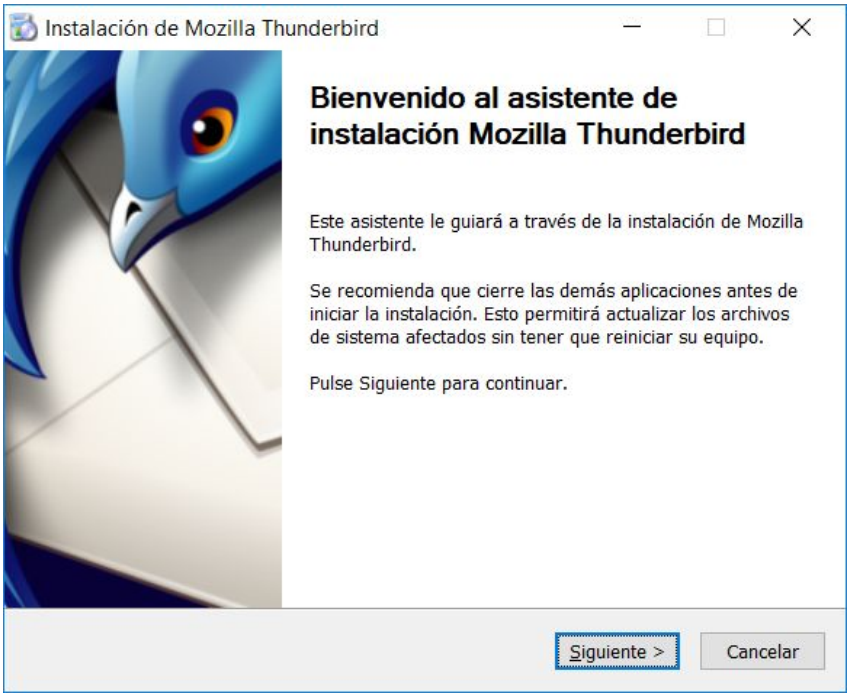
36. Hay que pinchar en el botón "**Descarga gratuita**" y el archivo ejecutable comenzará a descargarse:



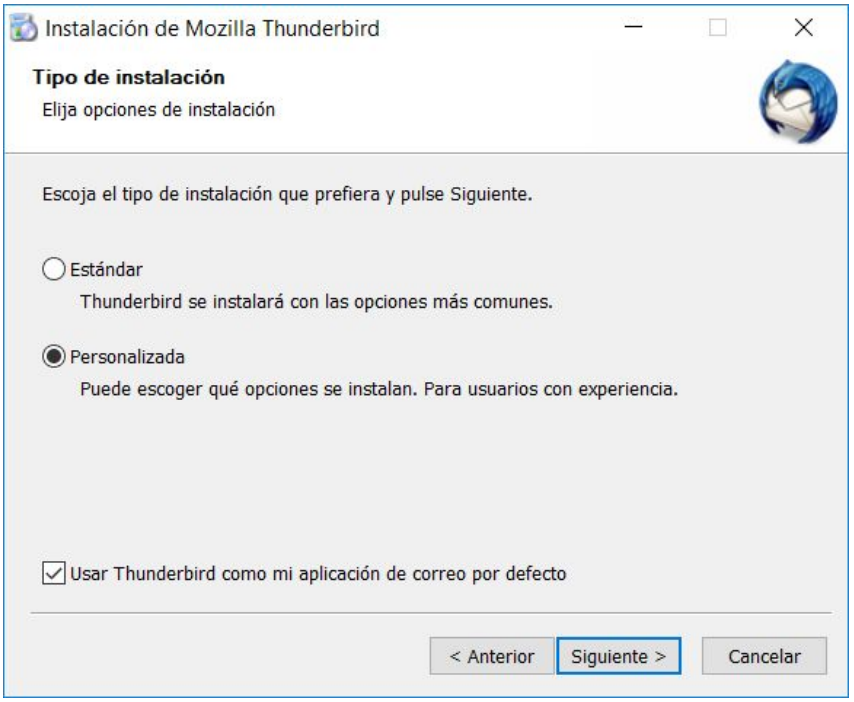
37. Una vez finalice la descarga, en la carpeta de Descargas aparecerá un archivo ejecutable llamado **Thunderbird Setup 52.4.0.exe**. Para instalarlo hay que hacer doble click en él. Se pulsa el botón "**Ejecutar**":



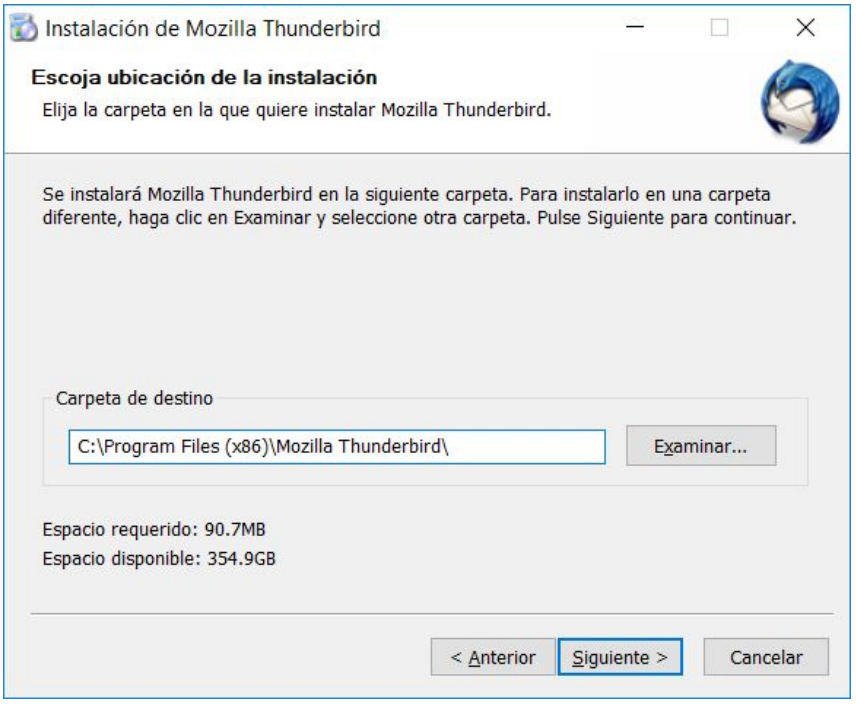
38. Pulsar el botón “Siguiente”:



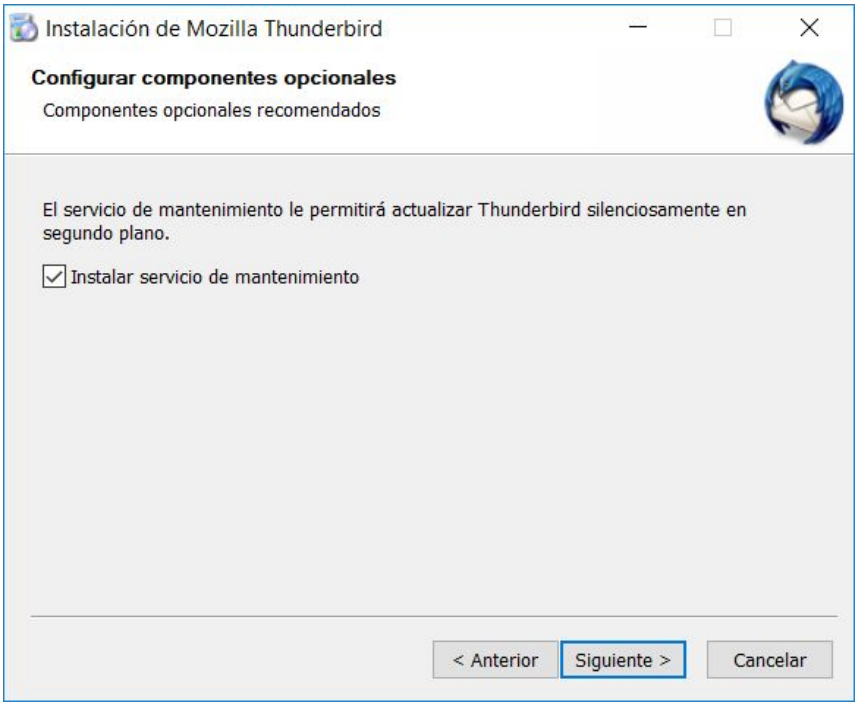
39. Se selecciona la opción “**Personalizada**” y se pulsa el botón “**Siguiente**”:



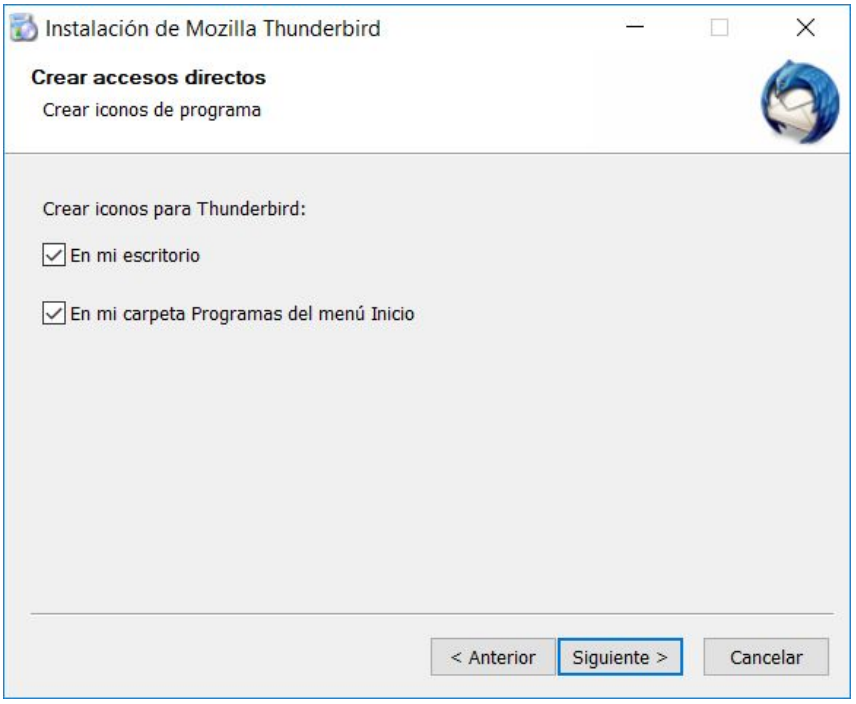
40. Se elige una ruta donde instalar Thunderbird se pulsa el botón “**Siguiente**”:



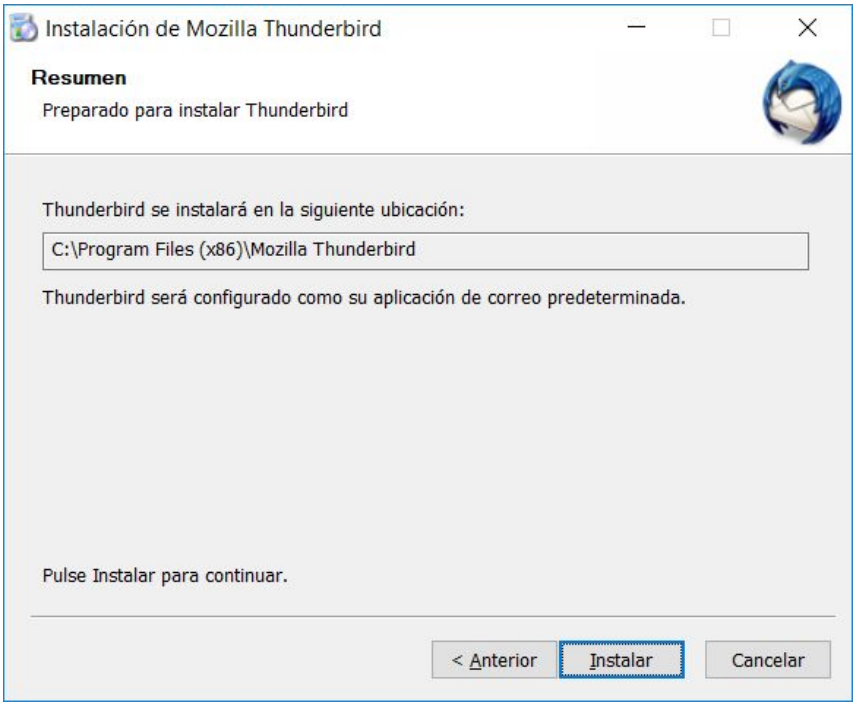
41. Se pulsa el botón “**Siguiente**”:



42. Se pulsa el botón “**Siguiente**”:

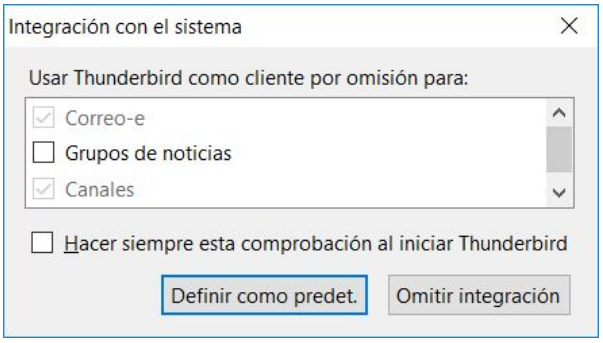


43. Se pulsa el botón “**Instalar**”:

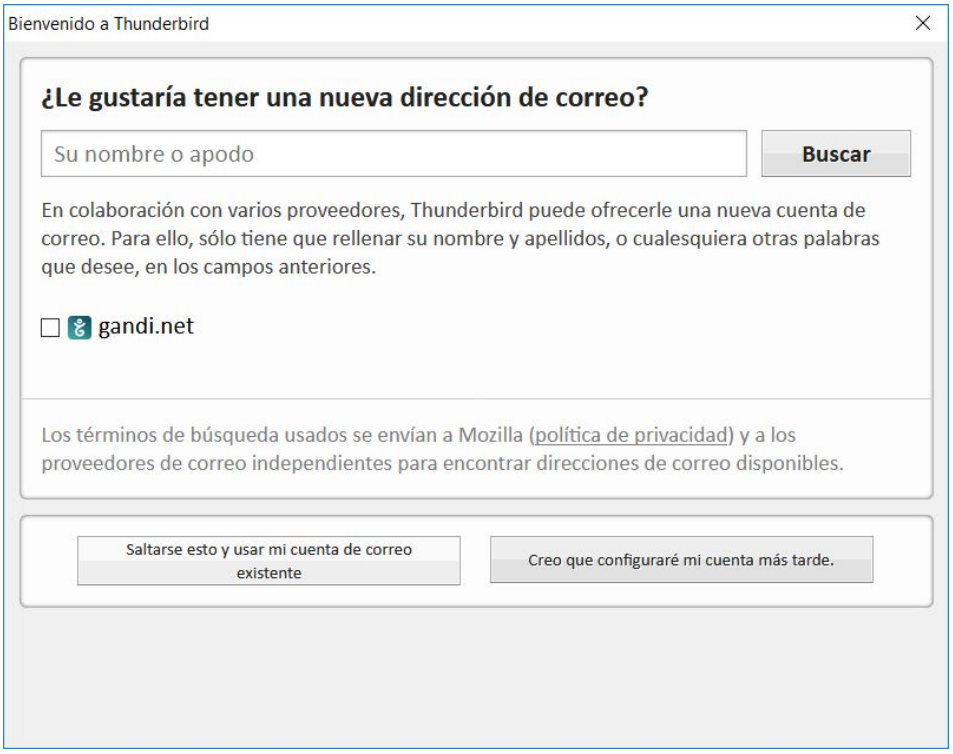


44. Se pulsa el botón “Finalizar”:

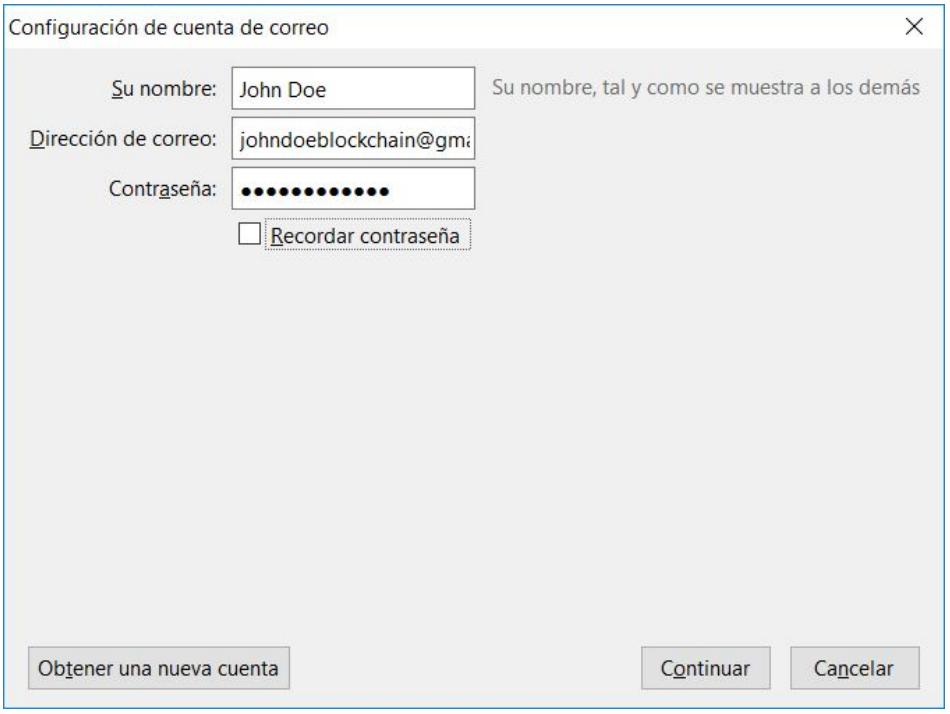
45. Pulsar el botón “**Omitir integración**”:



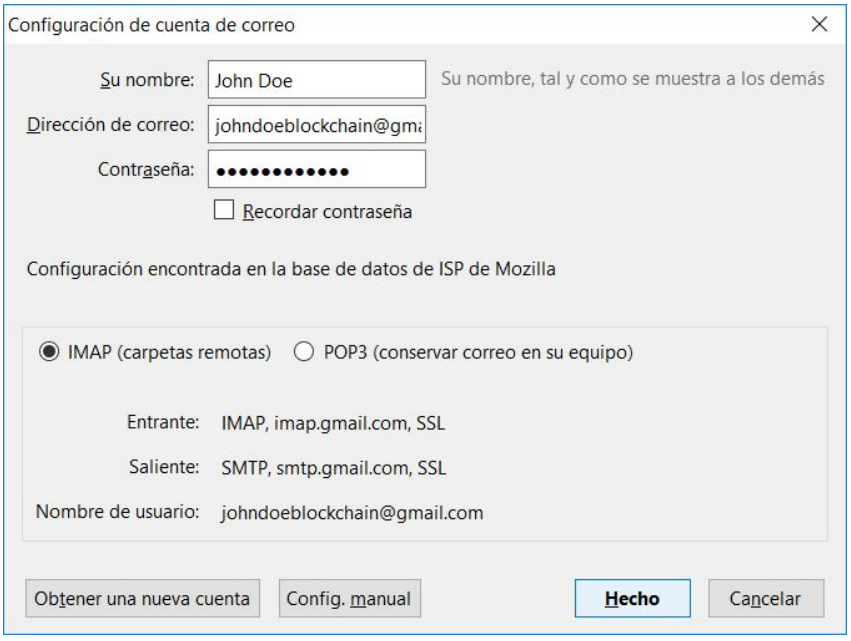
46. Desactivar el checkbox “**gandi.net**” y pulsar sobre el botón “**Saltarse esto usar mi cuenta de correo existente**”:



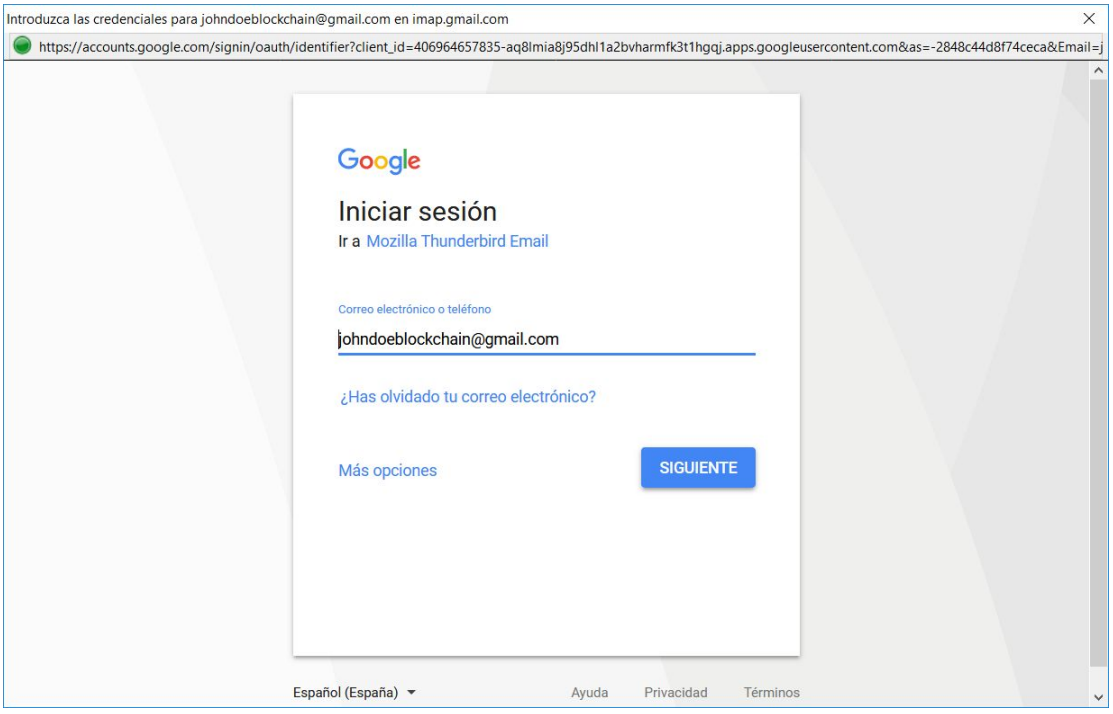
47. Se introducen los datos de la cuenta de mail existente. Dejar activada la opción de “**Recordar contraseña**” se deja a voluntad del usuario, pero no se recomienda en ningún caso. Se pulsa el botón “**Continuar**”:



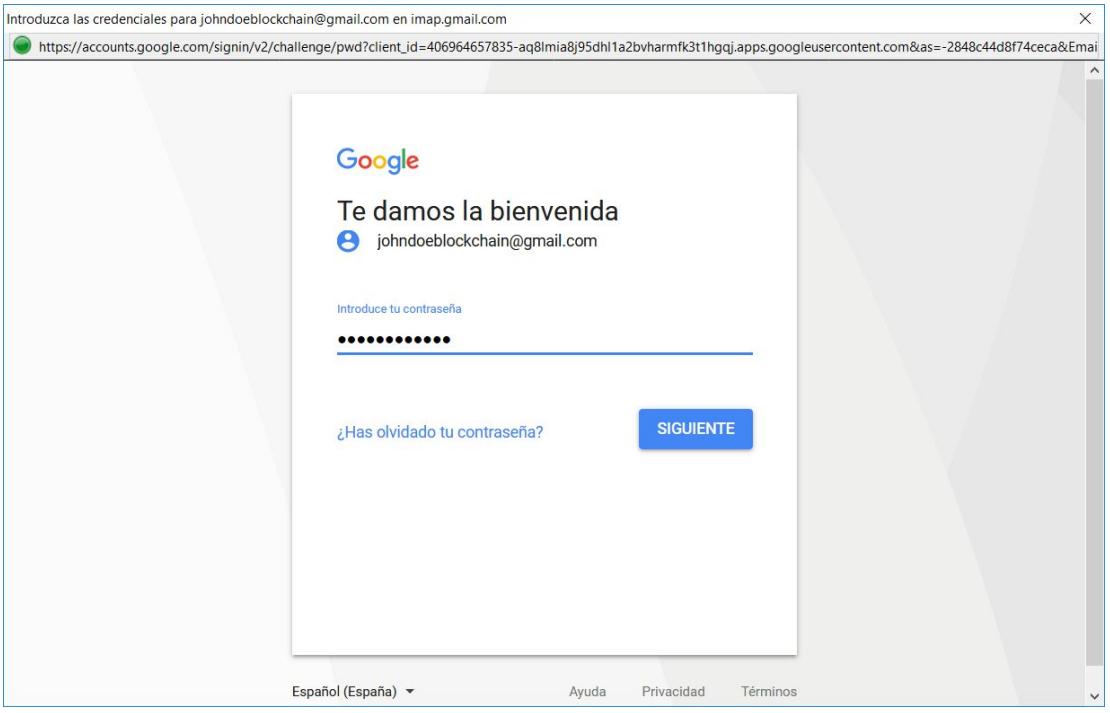
48. Se auto completará la configuración automáticamente. Se pulsa el botón “**Hecho**”:



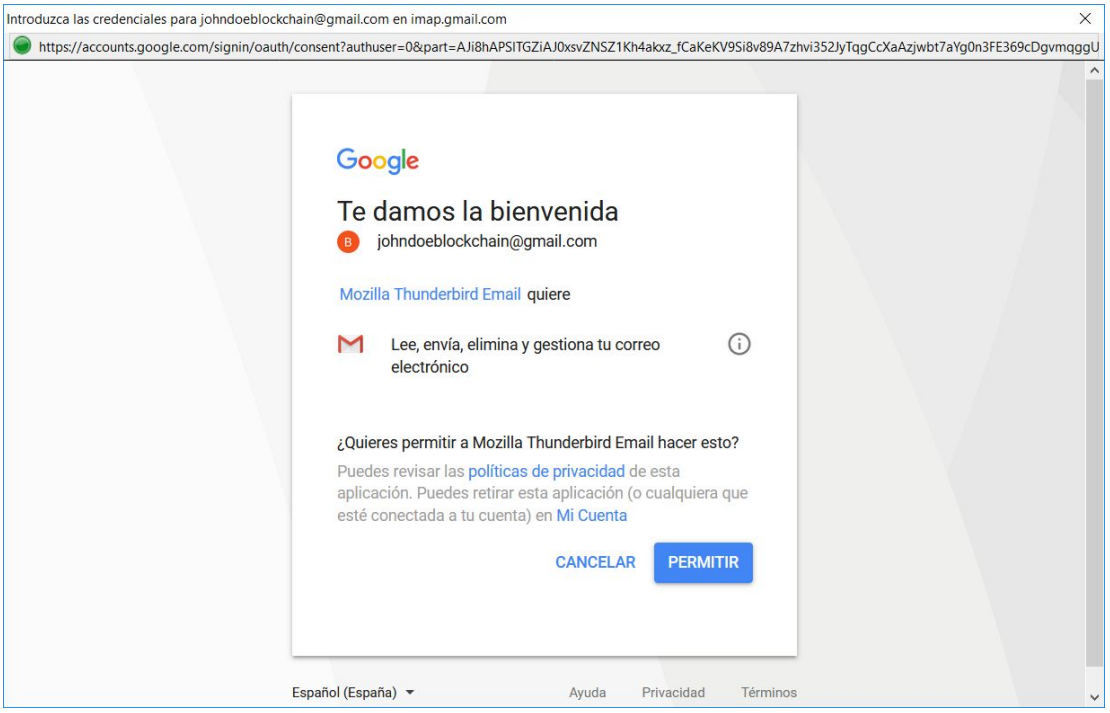
49. En el ejemplo se ha usado una cuenta de correo de Gmail, en este caso se abrirá una ventana de un navegador para introducir las credenciales de la cuenta de correo. Se pulsa el botón “**Siguiente**”:



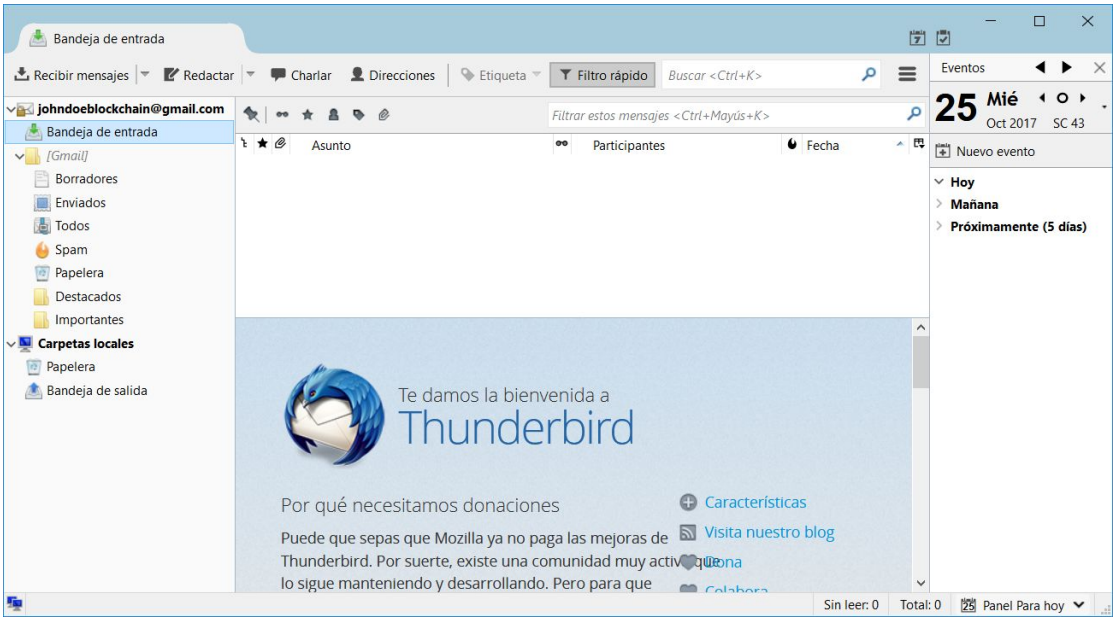
50. Y la password del correo de Gmail. Se pulsa el botón “**Siguiente**”:



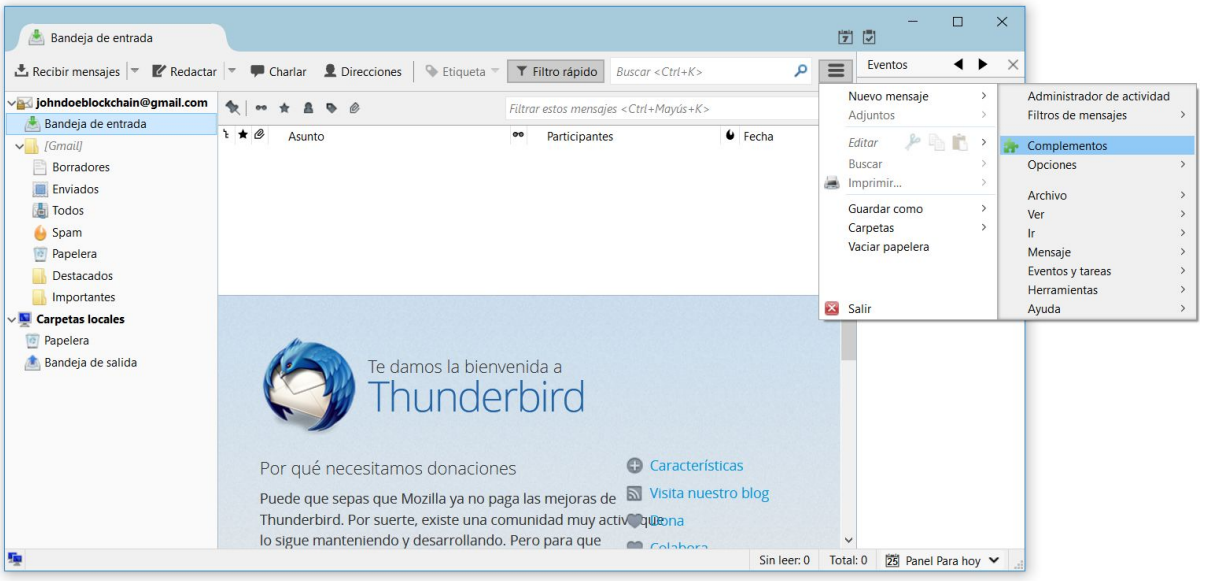
51. Se pulsa el botón “**Permitir**”:



52. Ya está instalado y configurado el cliente de correo Thunderbird. Se puede ir a la bandeja de entrada y comprobar que se reciben y envían correos:



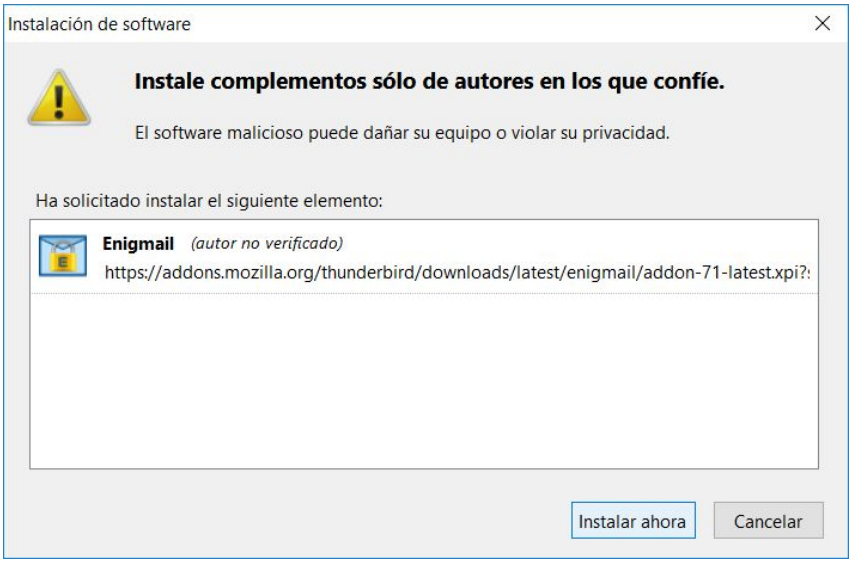
53. Ahora solo falta instalar **Enigmail**, se trata de un complemento de Thunderbird que permite acceder a las funciones de encriptación de GnuPG desde dentro de Thunderbird. Para ello, desde Thunderbird hay que pinchar en el botón que se muestra en la siguiente imagen y luego en la opción "**Complementos**":



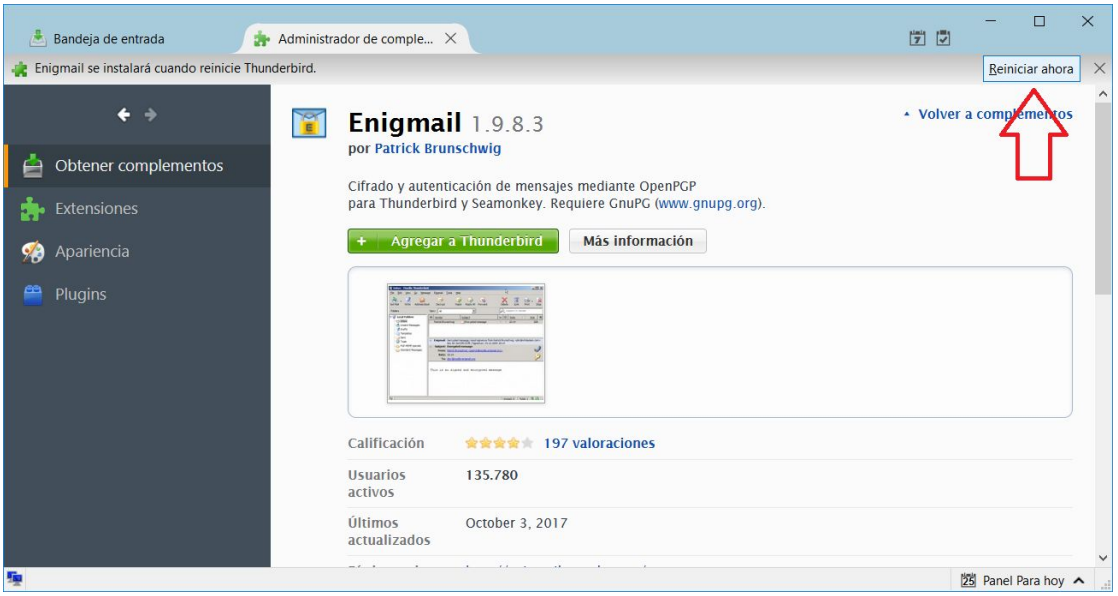
54. En “**Obtener complementos**”, más abajo aparece entre los complementos más destacados **Enigmail**:

55. Pulsar el botón “**Agregar a Thunderbird**”:

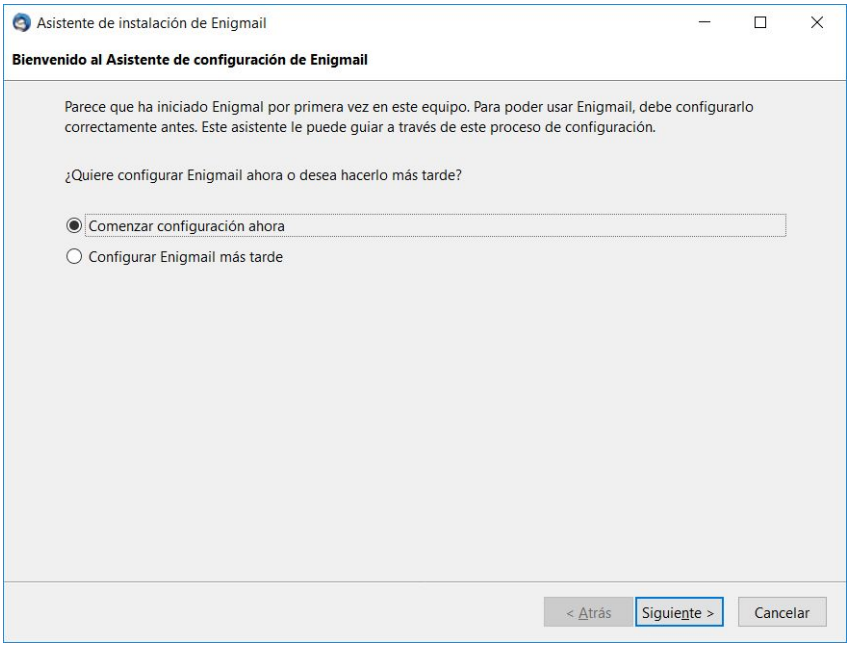
56. Pulsar el botón “**Instalar ahora**”:



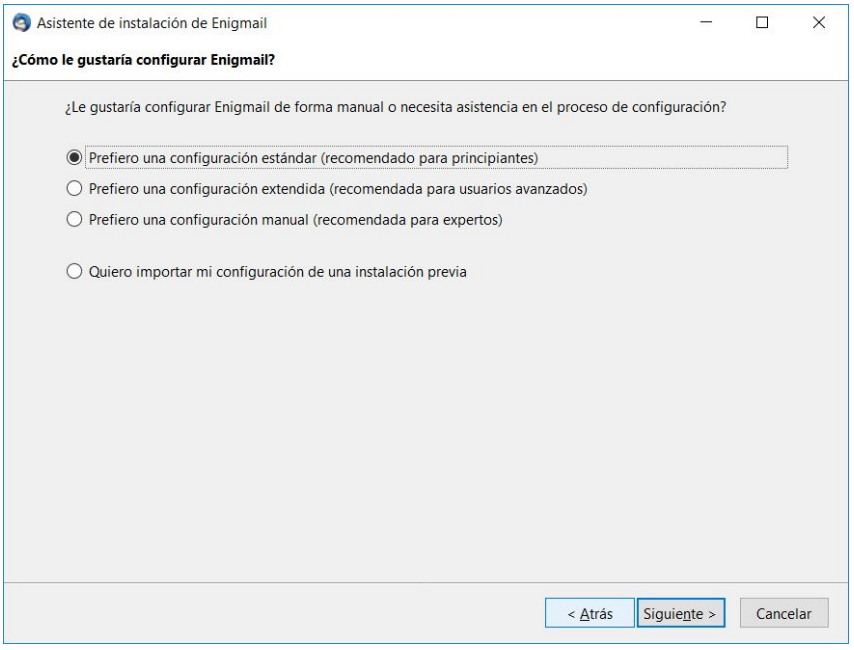
57. Pulsar el botón “**Reiniciar ahora**” que aparece en la parte superior derecha de Thunderbird:



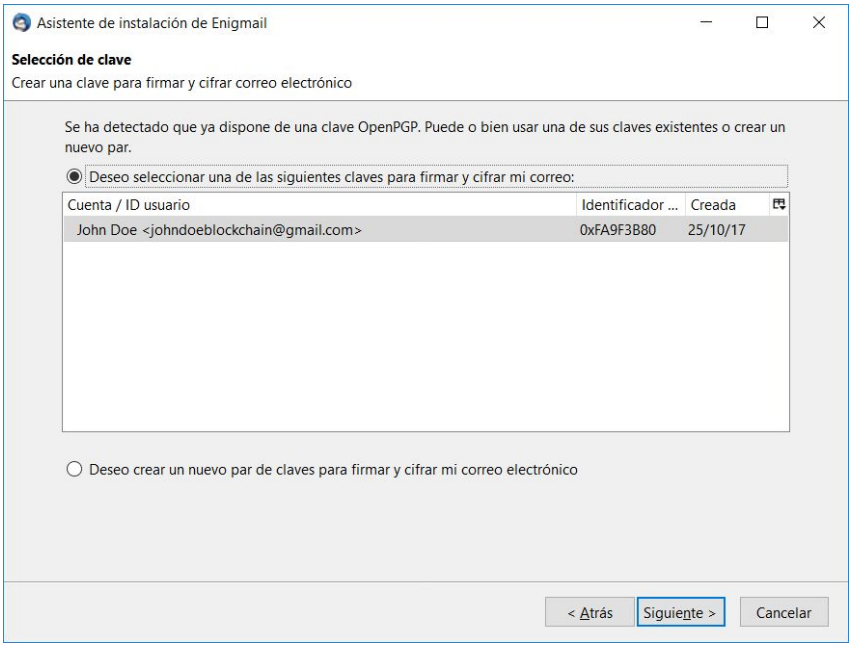
58. Se abrirá el asistente de configuración de Enigmail. Se selecciona la opción "**Comenzar configuración ahora**" y se pulsa el botón "**Siguiente**":



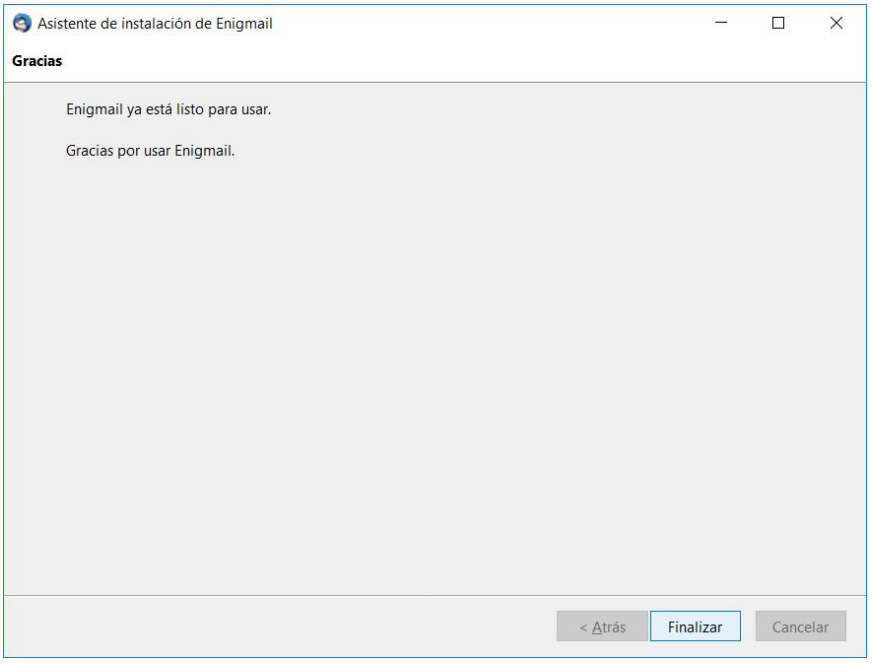
59. Se selecciona la opción "**Prefiero una configuración estándar (recomendado para usuarios principiantes)**" y se pulsa el botón "**Siguiente**":



60. Se selecciona la clave que automáticamente lee de GnuPG que hemos instalado y configurado al inicio de este documento y se pulsa el botón “**Siguiente**”:



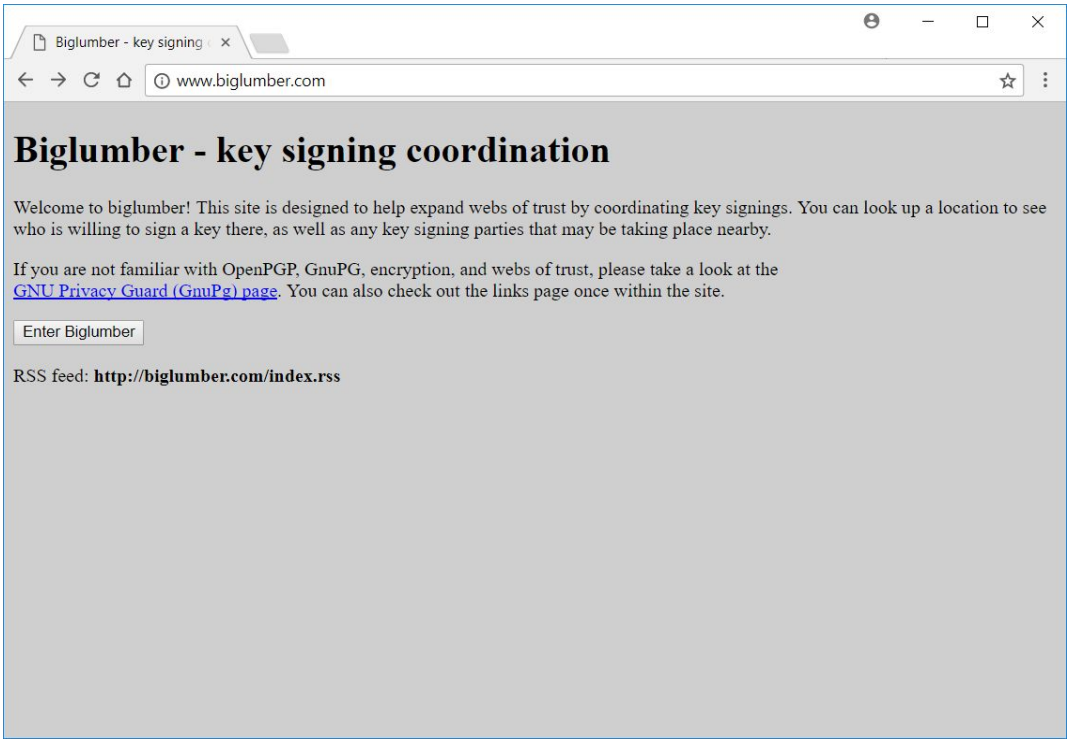
61. Y finalmente se pulsa el botón “**Finalizar**”:



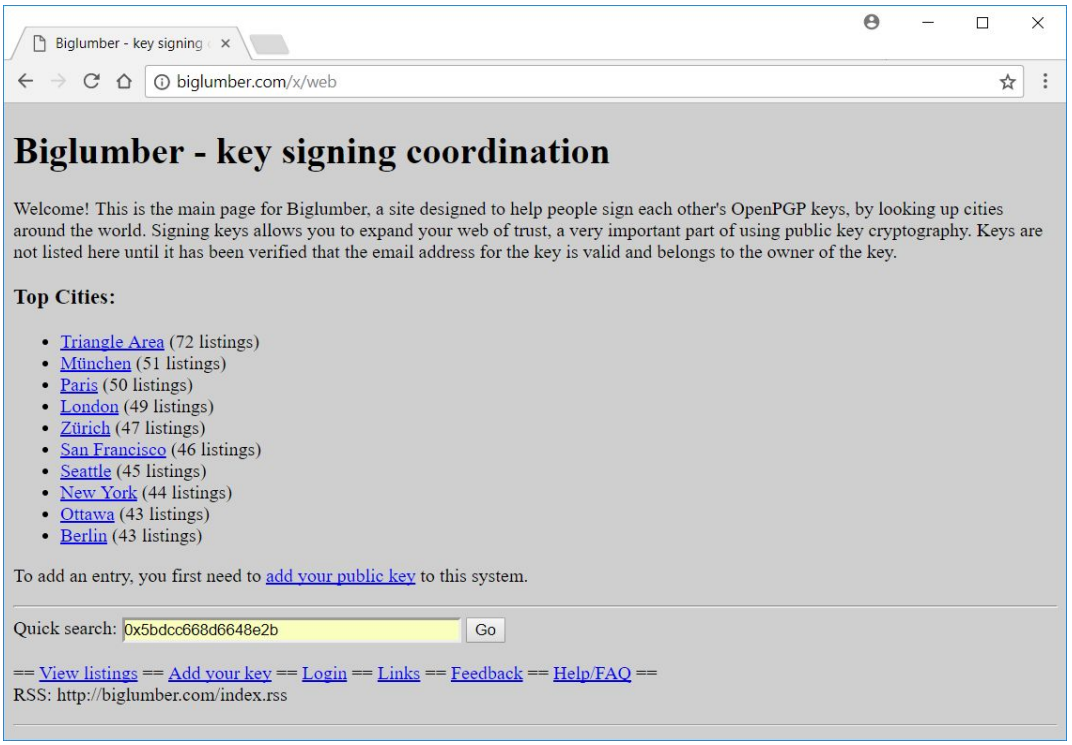
62. Antes de probar a mandar un mail cifrado a alguien primero debemos añadir la clave pública de ese “alguien” a GnuPG, para ello primero hay que ir a la siguiente URL:

    http://www.biglumber.com

    y pulsar el botón “**Enter Biglumber**”:

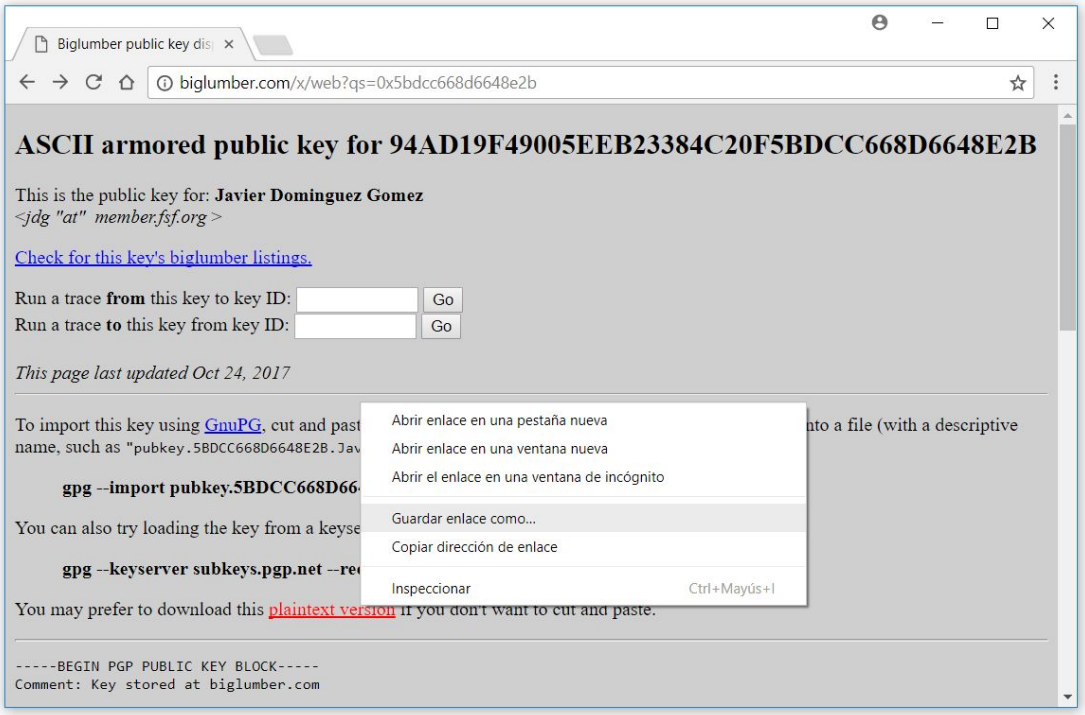


63. Una vez dentro buscar la clave pública, por ejemplo, de Javier Dominguez Gomez mediante la siguiente cadena hexadecimal: **0x5bdcc668d6648e2b**

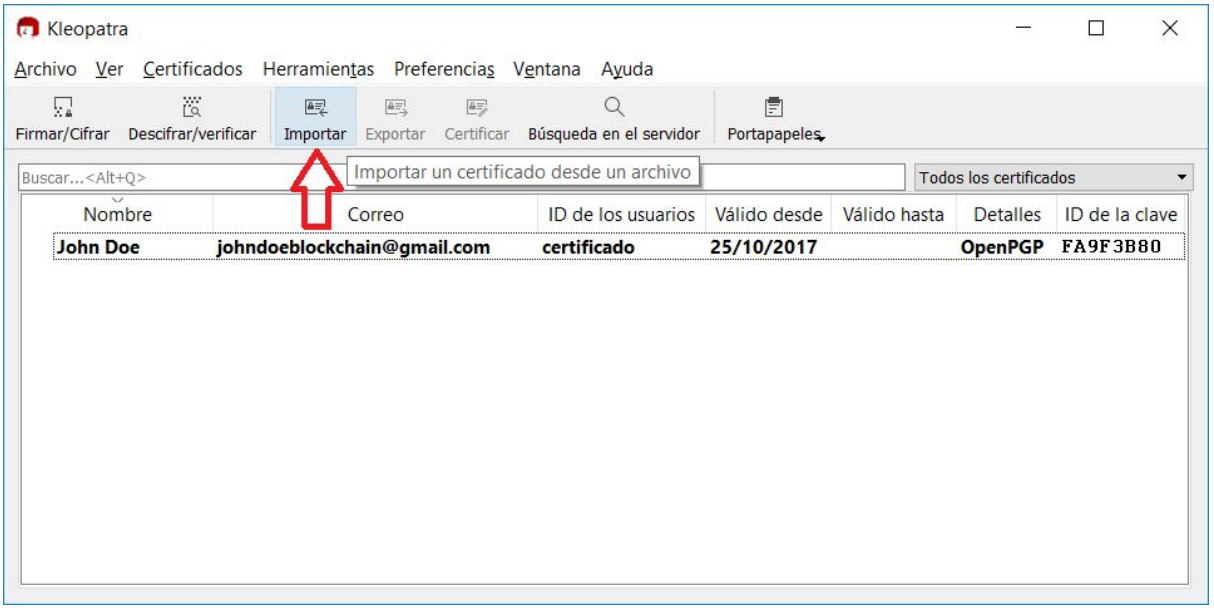


y pulsar el botón “**Go**”.

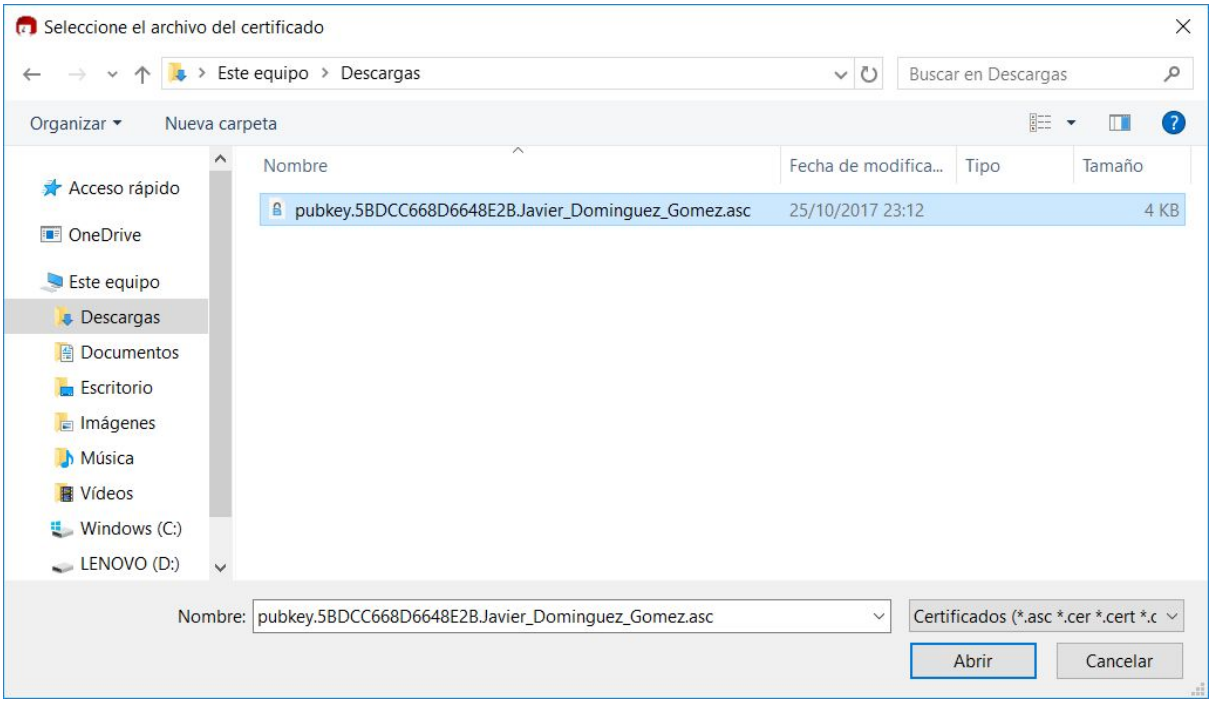
64. Descargar en archivo de texto plano la clave pública de Javier Domínguez Gómez, para ello hay que hacer click con el botón derecho del ratón sobre el link "**plaintext version**", seleccionar la opción "**Guardar enlace como…**" y guardarlo en alguna carpeta local, por ejemplo "**Descargas**".



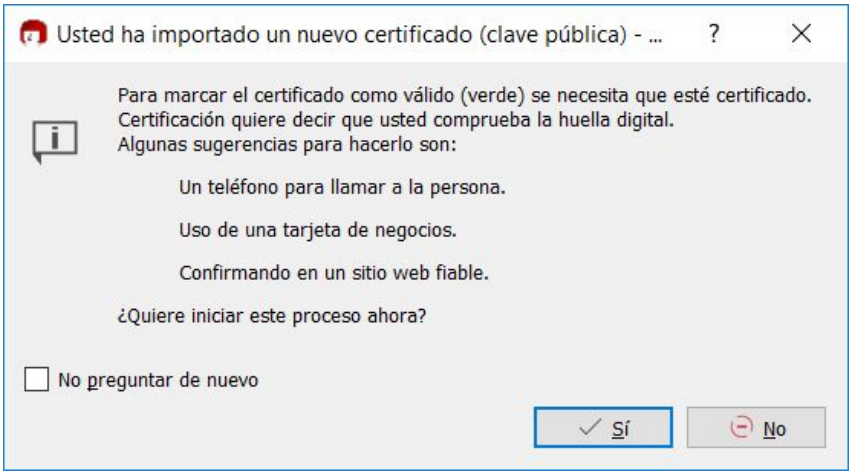
65. Una vez descargada la la clave pública hay que ir a Kleopatra de nuevo y pulsar el botón "**Importar**".



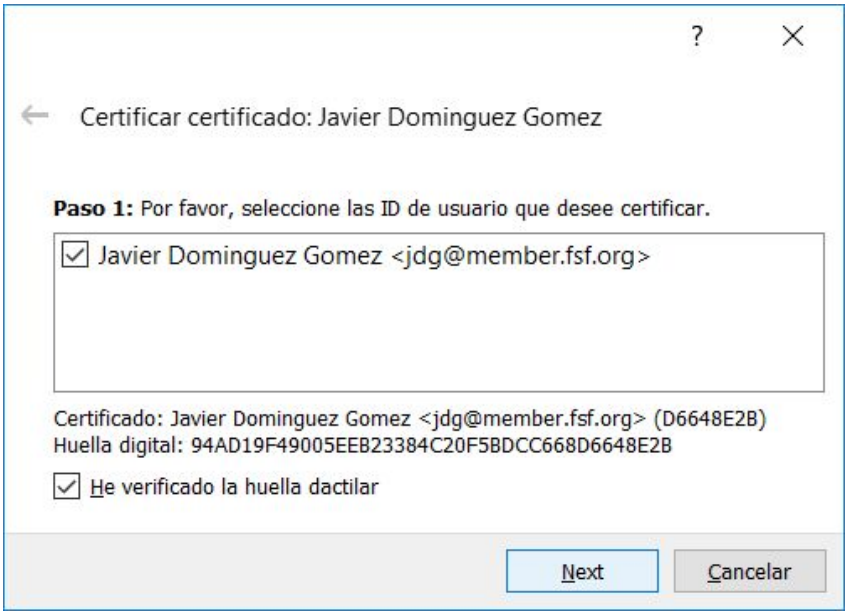
66. Hay que ir a la carpeta donde se descargó la clave pública con extensión *.asc*, seleccionarla y pulsar el botón "**Abrir**":



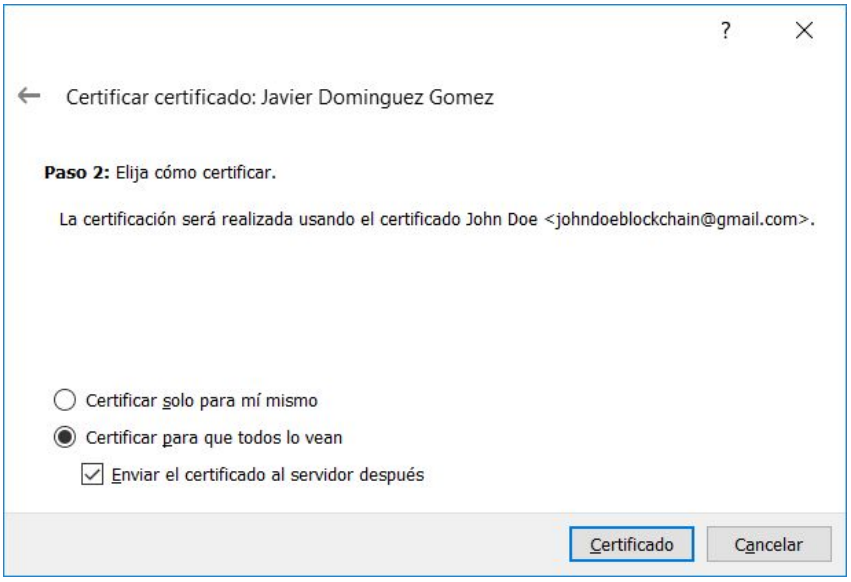
67. Aparecerá una ventana con una serie de indicaciones y buenas prácticas a la hora de añadir nuevas claves públicas. En este caso se pulsa el botón "**Sí**":



68. Una buena práctica es verificar previamente con el dueño de la clave pública que se quiere importar la huella digital o *fingerprint* del mismo, en este caso os lo doy por aquí (véase en la imágen donde pone "*Huella digital:*") o si queréis me lo podéis preguntar por Telegram (*@xe26505*), por twitter (*@ingenieriainv*) o en persona quedando conmigo en una *Key signing party* o cualquier otra circunstancia. Para seguir con la guía habría que activar los do checkboxes y pulsar el botón "**Next**":



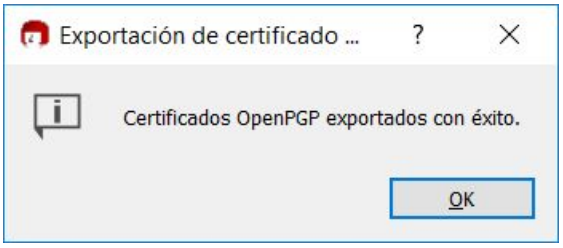
69. En esta pantalla se puede seleccionar la opción "**Certificar para que todos lo vean**", "**Enviar el certificado al servidor después**" y pulsar el botón "**Certificado**":



70. Aparecerá una ventana pidiendo la password del certificado que se ha creado al inicio de esta guía:

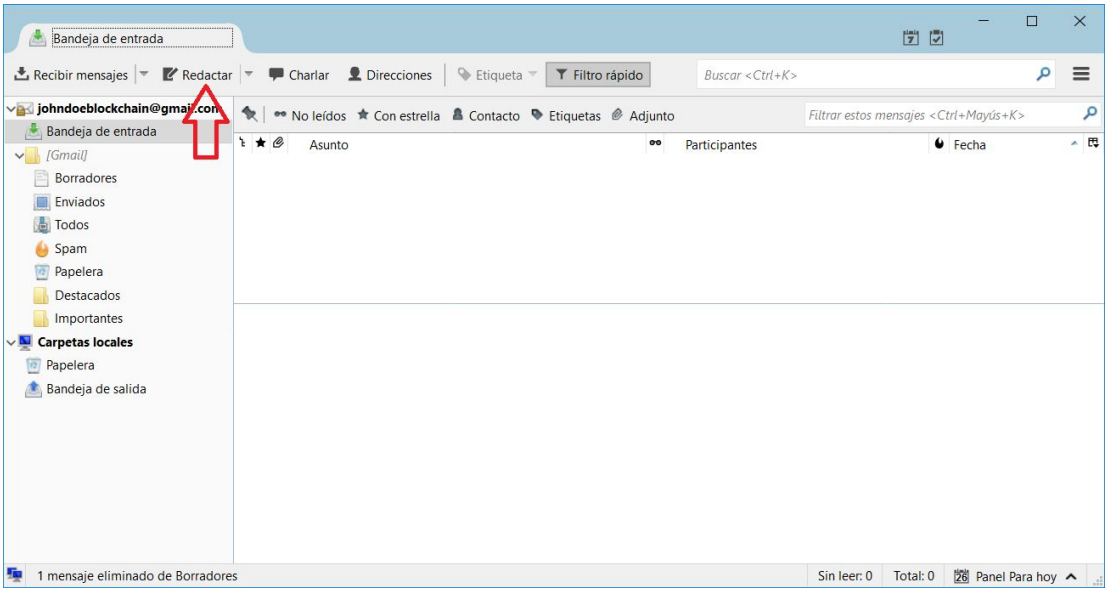
71. Pulsar el botón "**Continuar**":

72. Pulsar el botón "**OK**":

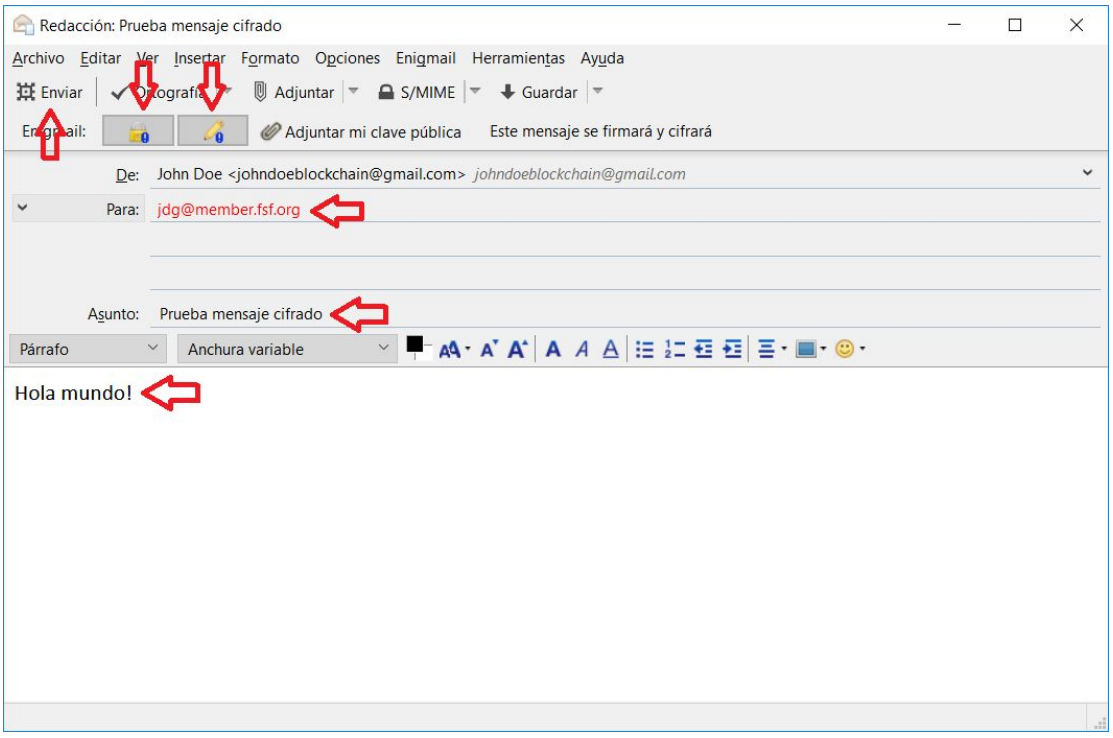


73. Pulsar el botón Terminar:

74. Una vez descargado e importado la clave pública de Javier Domínguez Gómez (jdg@member.fsf.org) se ha de probar el envío de un mail cifrado a su cuenta de correo electrónico. Para ello hay que pulsar el botón "**Redactar**" en Thunderbird:

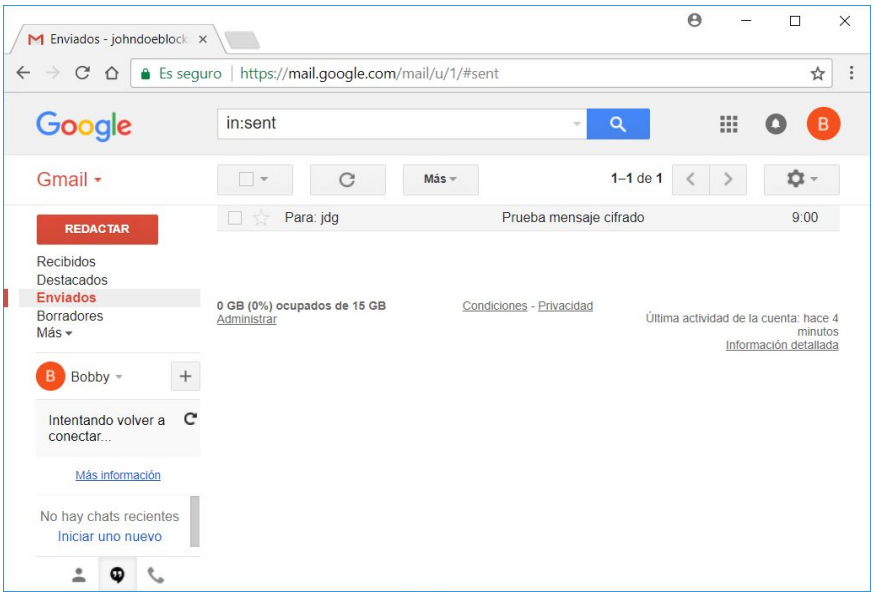


75. Primero se ha de pulsar los dos botones de la parte superior, el del **candado** para cifrar, y el del **lápiz** para firmar. Luego se escribe en el campo "**Para:**" la dirección de mail jdg@member.fsf.org, en el campo "**Asunto:**" por ejemplo "*Prueba mensaje cifrado*" y en el cuerpo del mail un texto legible cualquiera, por ejemplo "*Hola mundo!*". Finalmente se pulsa el botón "**Enviar**":

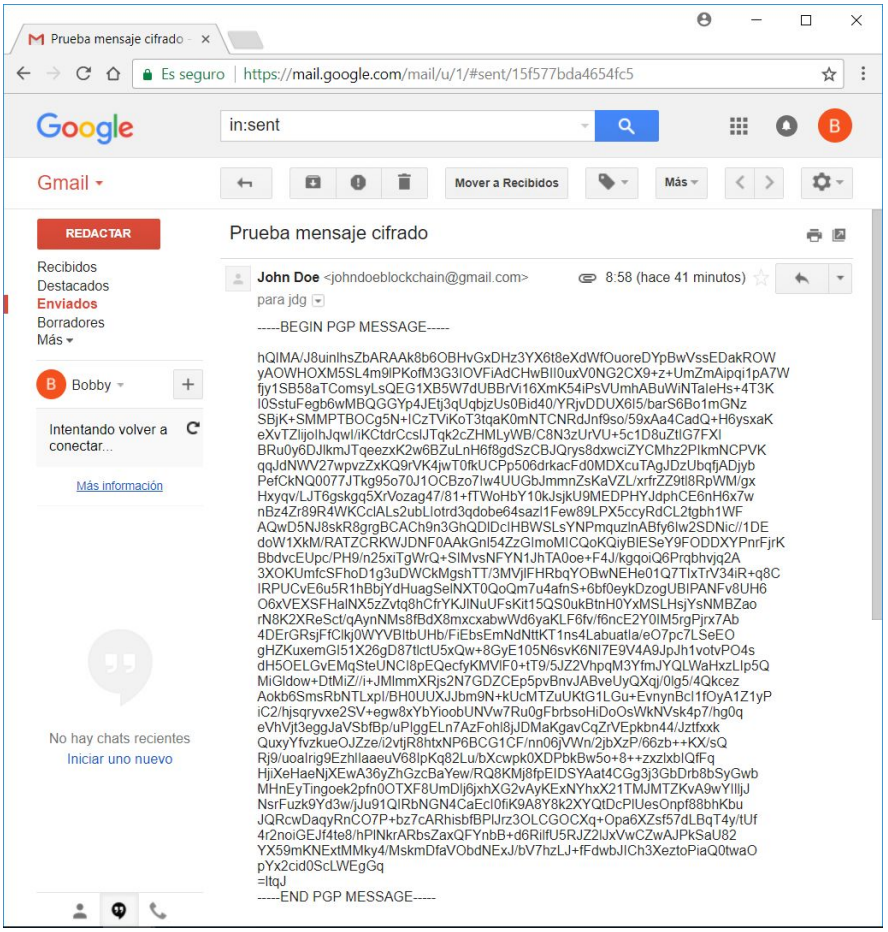


76. Aparecerá una ventana en la que pide introducir la password del certificado con el certificado personal, el de John Doe. Se introduce la password y se pulsa el botón "**OK**":

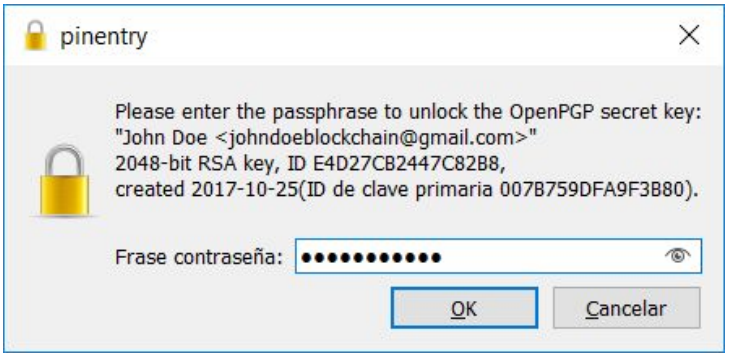
77. Una manera de ver cómo se ha enviado este mail cifrado desde la cuenta de Gmail johndoeblockchain@gmail.com a la cuenta de mail de Javier Domínguez Gómez jdg@member.fsf.org es yendo a la página de Gmail, hacer login, pinchar en elementos enviados y luego en el mail enviado.



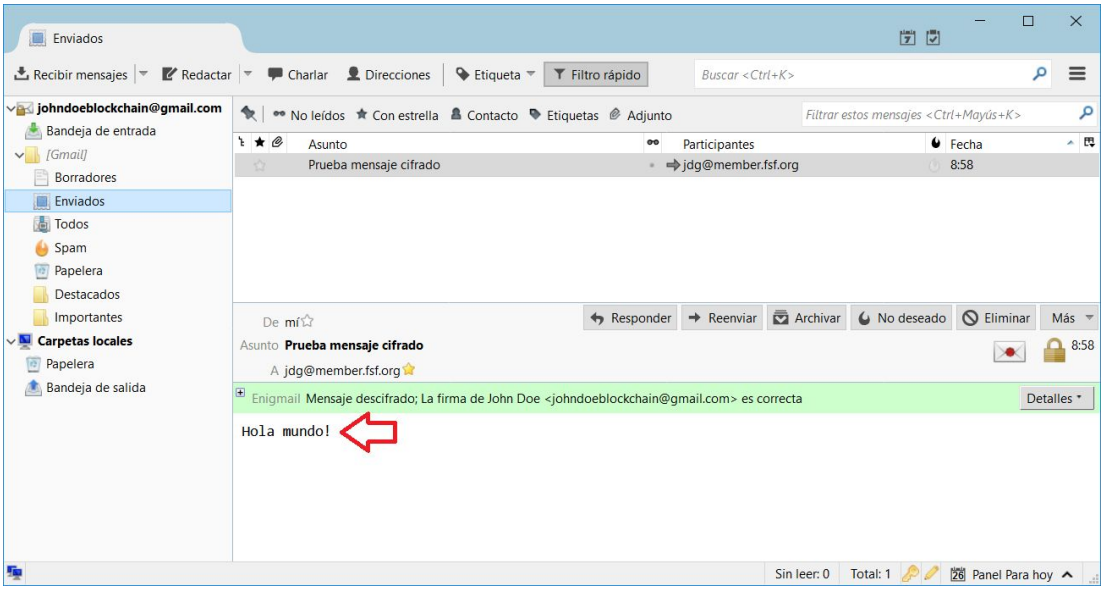
78. Aparecerá un texto encriptado, ese texto es el mensaje "*Hola mundo!*" otros datos más cifrados. Esto sucede porque el cliente de correo web de Gmail no utiliza por defecto el software GnuPG que hay instalado en el ordenador local con las claves importadas:



79. Sin embargo, si se consulta la carpeta “**Enviados**” en Thunderbird y se selecciona el mail que se ha enviado encriptado, aparecerá automáticamente una ventana que pide introducir la password del certificado de John Doe para poder desencriptar el mensaje:



80. Se introduce la password, se pulsa el botón “**OK**” y el mensaje aparecerá en texto claro:



81. Como último paso hay que comprobar con Javier Domínguez Gómez si ha recibido el mail, y si puede descifrarlo, para ello tendrá que importar la clave pública de John Doe en su GnuPG.