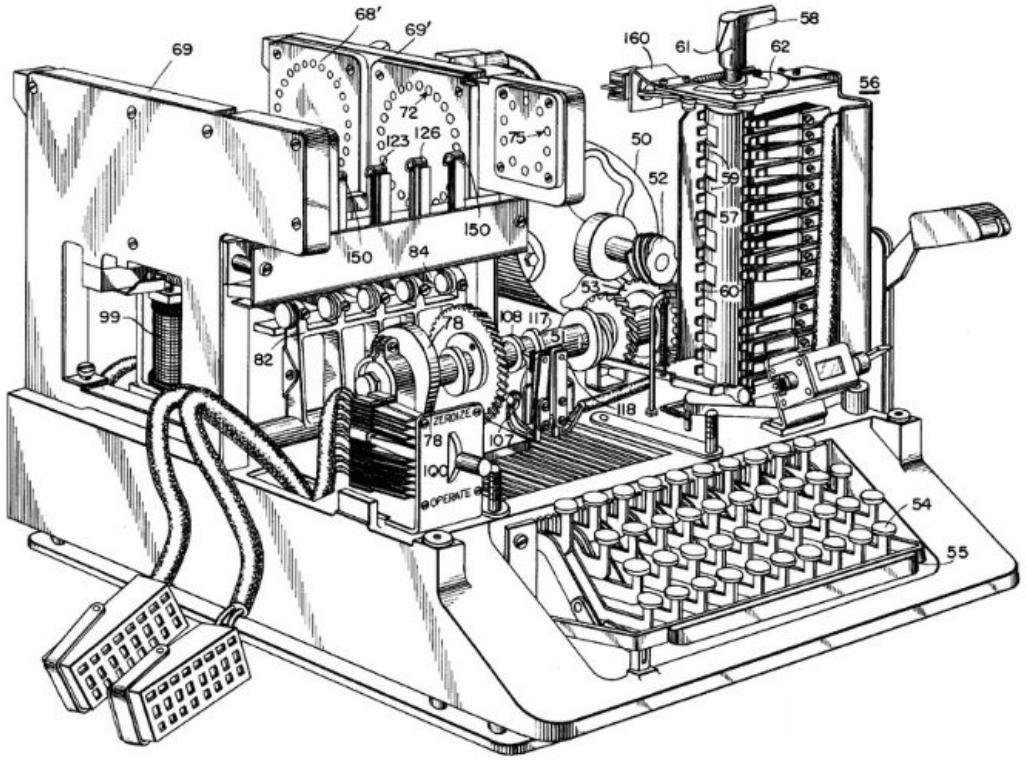
BLOCKCHAIN ESPAÑA

Guía de instalación
GnuPG + Thunderbird + Enigmail (Mac)



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

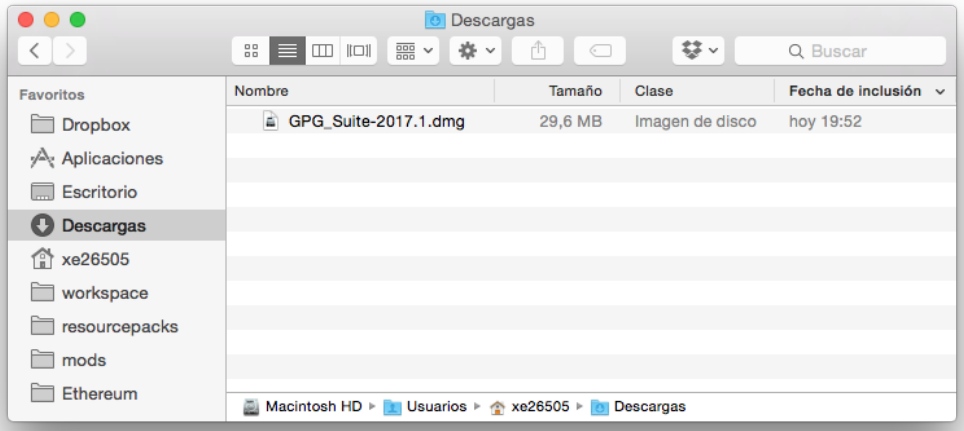
Este obra está bajo una licencia de:
Creative Commons Reconocimiento-NoComercial 4.0 Internacional.

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

   https://gpgtools.org/

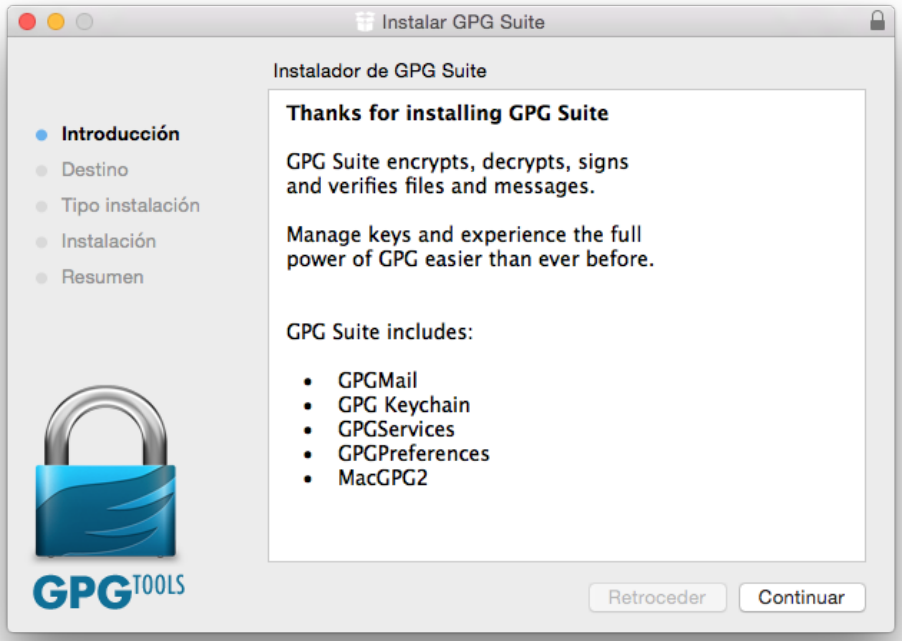
2. Hacer click en el botón "**Download GPG Suite**"

3. Se comenzará a descargar un archivo que se llama **GPG_Suite-2017.1.dmg** y se guardará en la carpeta "**Download**" o en la que se tenga por defecto para las descargas.

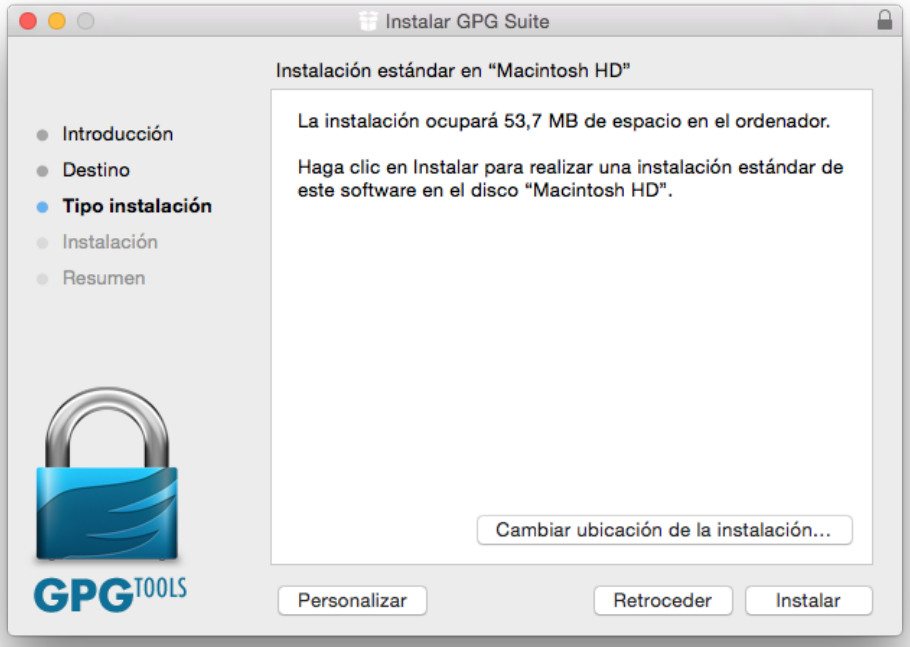


4. Hacer doble click para abrir el archivo. Se abrirá la siguiente pantalla. Para instalar la suite de GnuPG hay que hacer doble click sobre el icono que **install.pkg**:

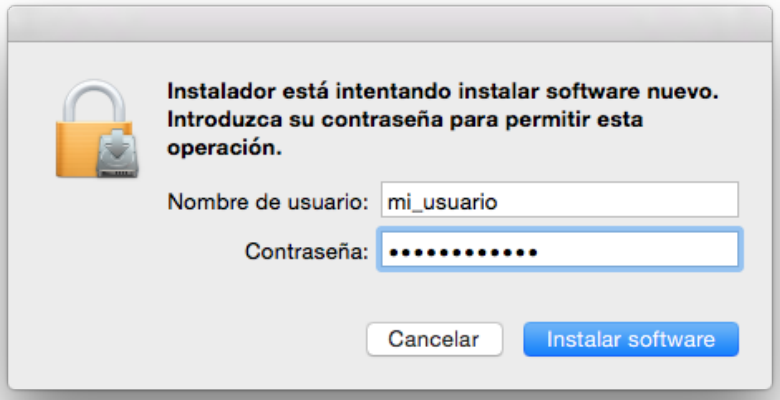
5. Se pulsa el botón “**Continuar**”:



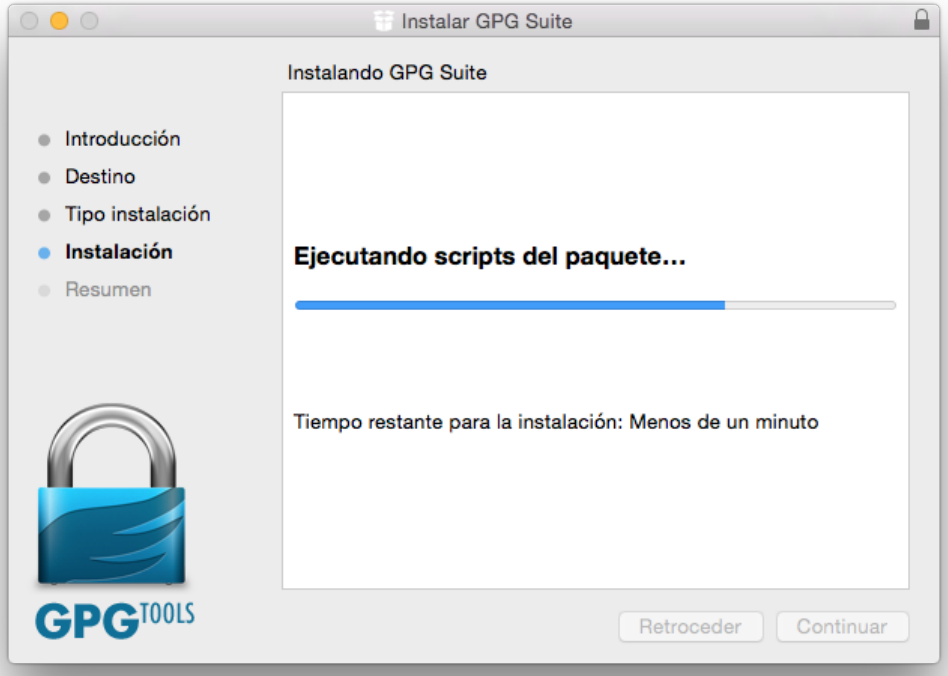
6. Se pulsa el botón “**Instalar**”.



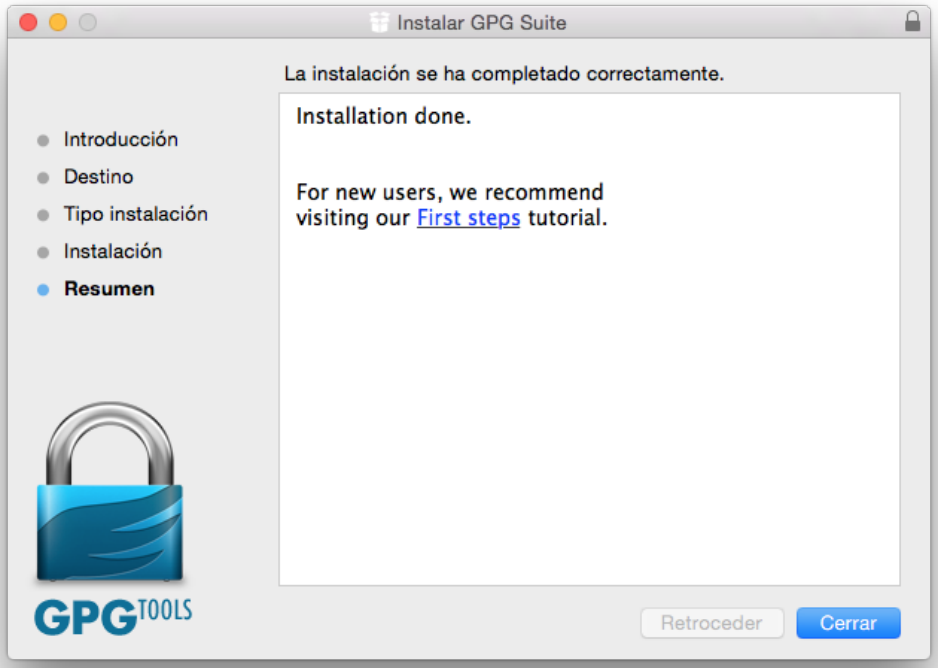
7. Probablemente pida introducir usuario y contraseña de administrador del Mac, luego pulsar el botón “**Instalar software**”. Sin no pide nada omitir este paso.



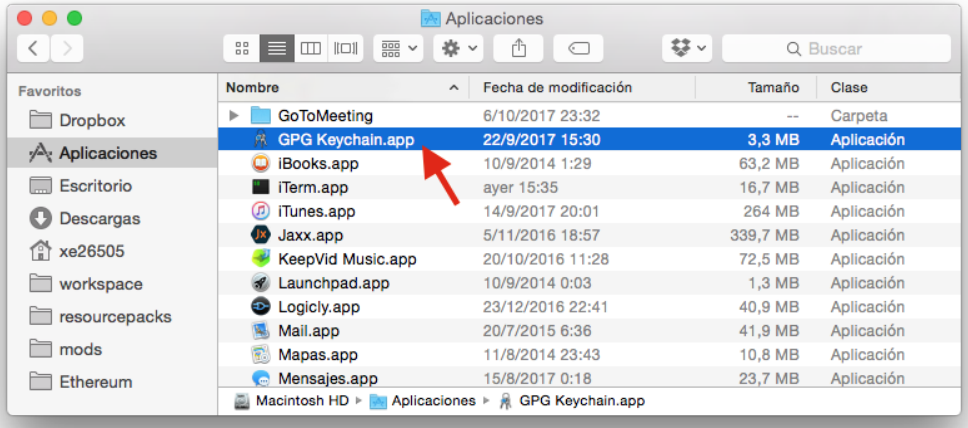
8. Comienza la instalación:



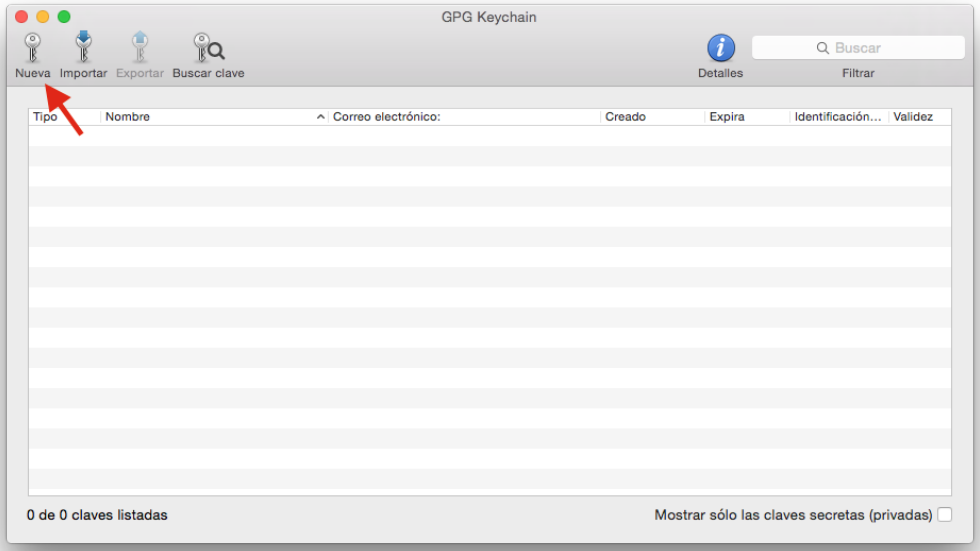
9. Cuando la instalación finalice se pulsa el botón “**Cerrar**”:



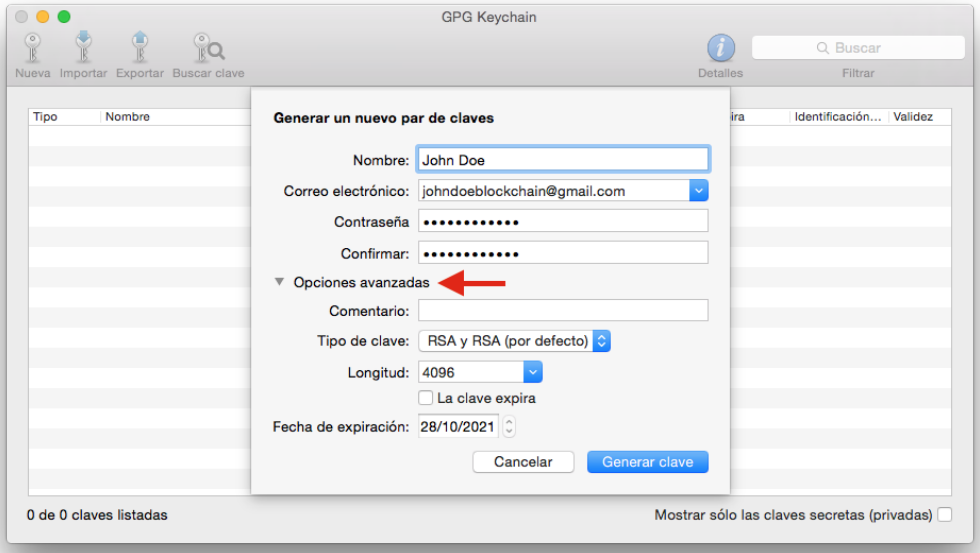
10. Una vez instalado hay que ir a la carpeta “**Aplicaciones**” y luego hacer doble click sobre “**GPG Keychain.app**” para abrir la aplicación:



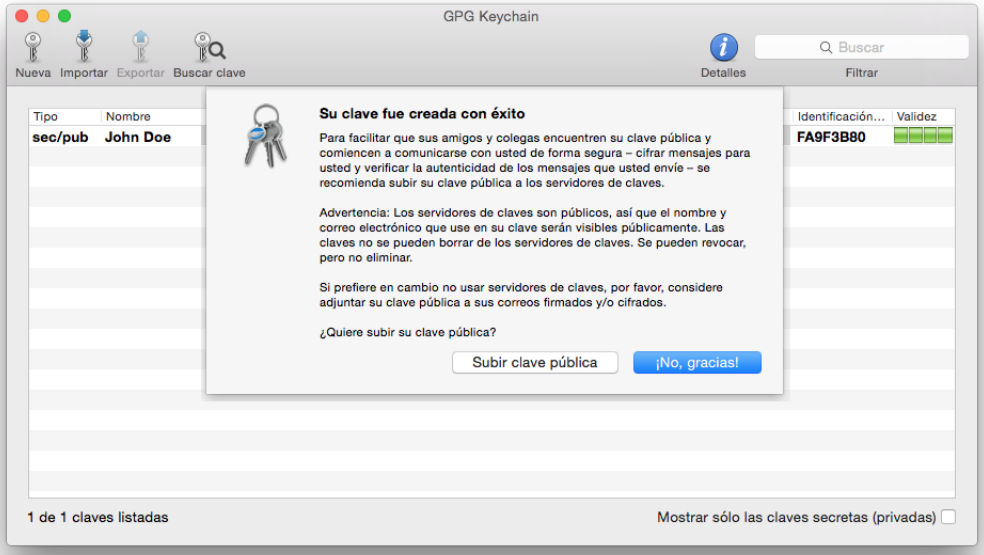
11. Lo primero que se ha de hacer es crear un par de claves (pública/privada), para ello hay que hacer click sobre el botón “**Nueva**”:



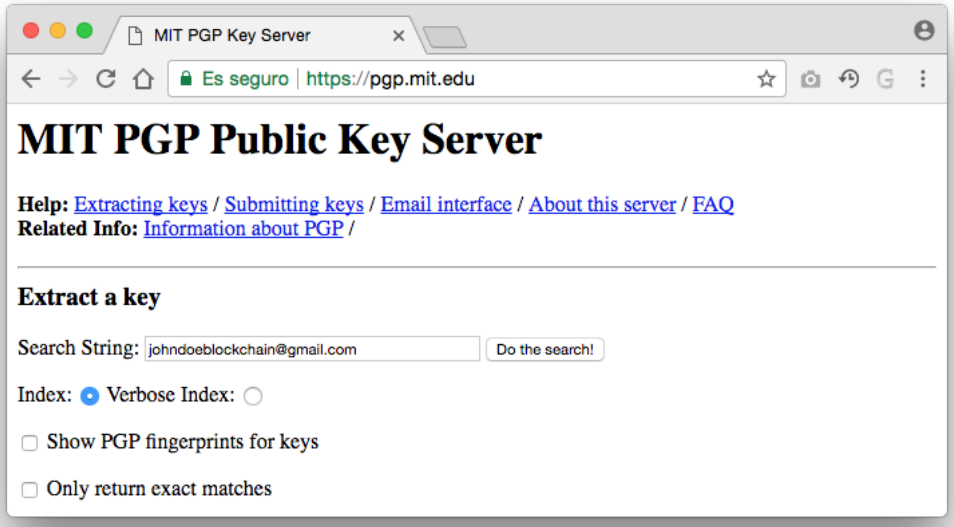
12. Hay que rellenar los campos, para el ejemplo se han elegido unos datos standard. Se puede pulsar en la opción “**Opciones avanzadas**” y elegir entre varios tipos de clave diferentes, la longitud de la misma y si la clave expira o no, para este ejemplo yo recomiendo usar el tipo de clave “**RSA y RSA (por defecto)**”, longitud “**4096**” y desactivar la opción de “**La clave expira**”. Finalmente se pulsa el botón “**Generar clave**”. Aparecerá un mensaje donde el programa pide mover el ratón y pulsar teclas aleatoriamente para generar bytes random:



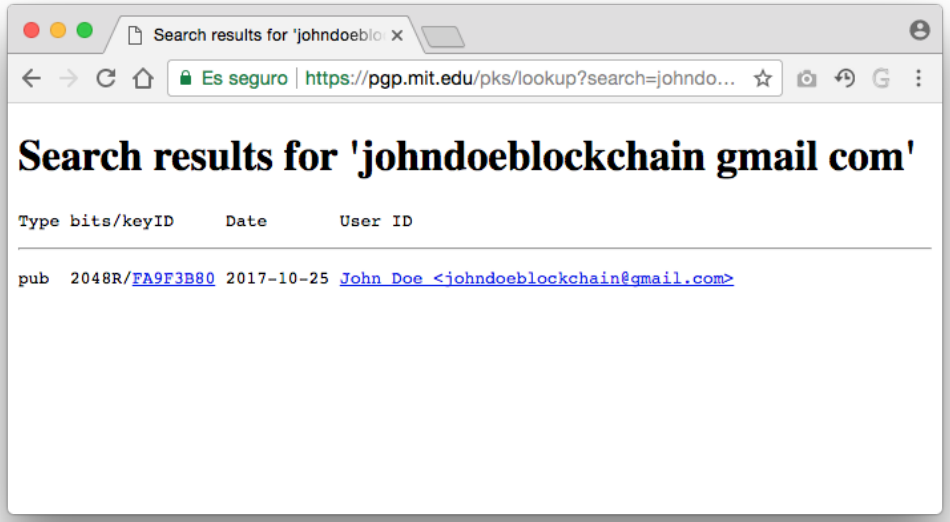
13. Una vez creadas el certificado que contiene el par de claves (pública/privada) se pulsa el botón "**Subir clave pública**" para subirla a los servidores de claves de internet:



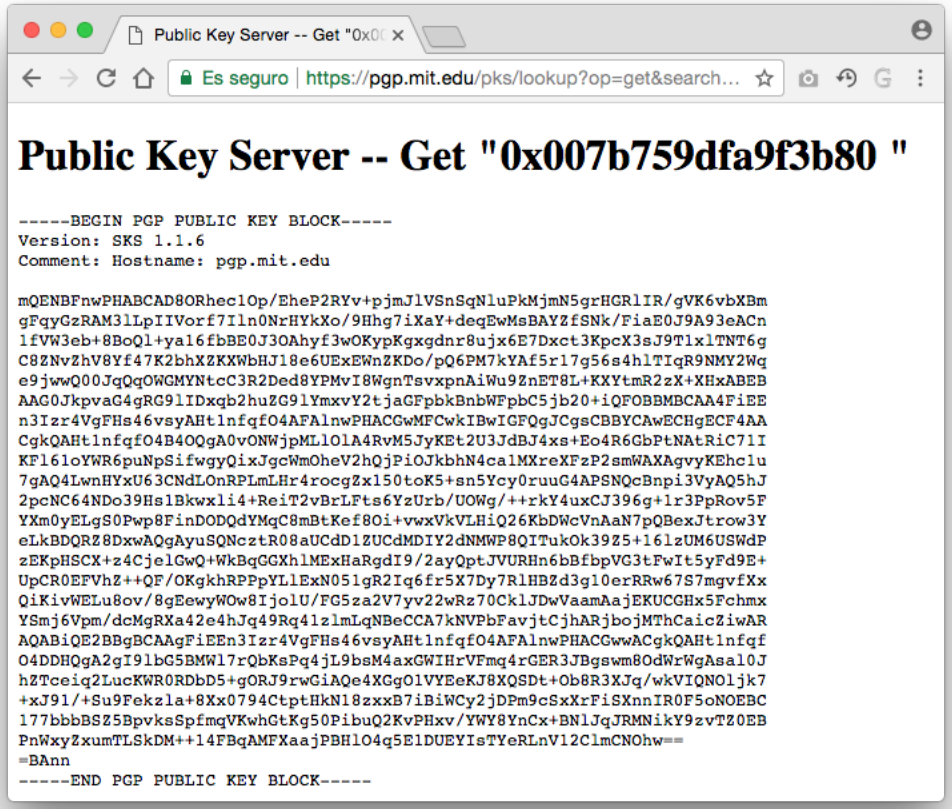
14. Finalmente hay que acceder a cualquiera de los servidores, por ejemplo a la URL: https://pgp.mit.edu y buscar la clave pública. Una manera sería introduciendo el email que se escogió a la hora de crear el par de claves:



15. Si todo ha salido correctamente aparecerá el certificado que se ha subido desde GPG Keychain.



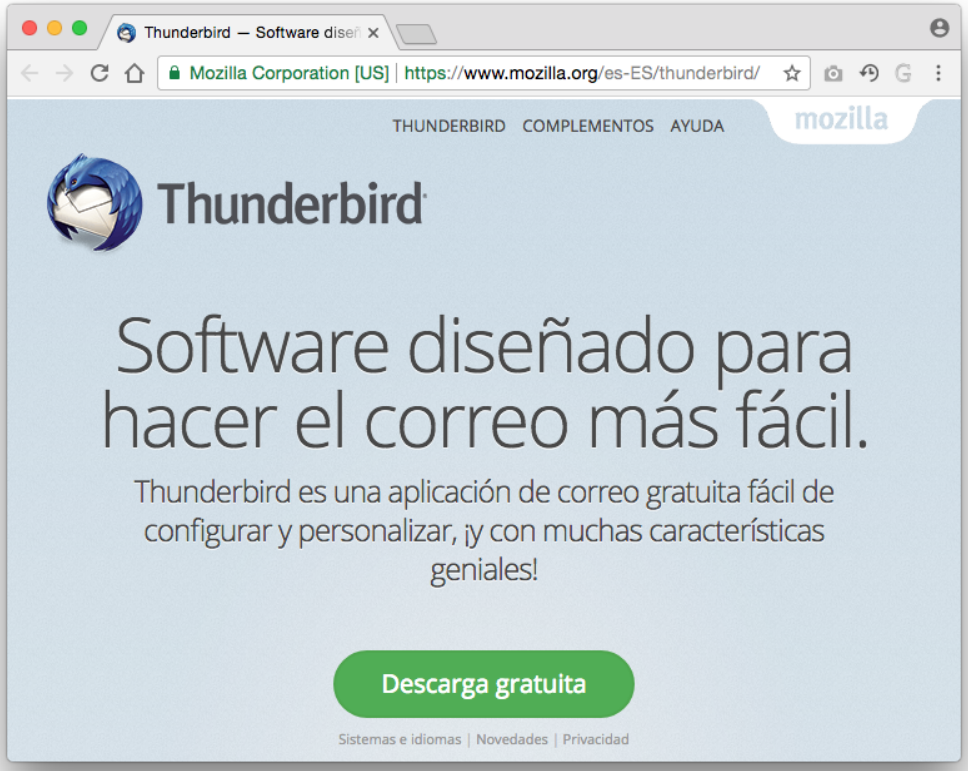
16. Al pinchar en el **keyID** se accede a una página donde aparece el texto que forma la clave pública:



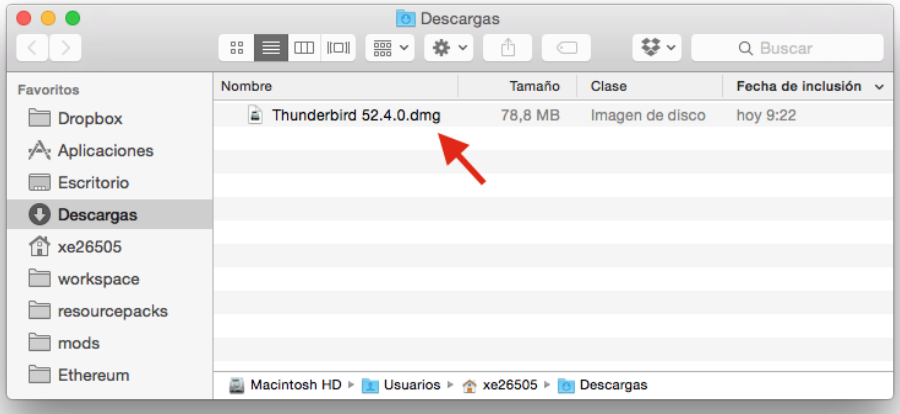
17. En este punto del documento se explica cómo descargar, instalar y configurar el cliente de correo Thunderbird. Hay que ir a la siguiente URL:

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

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

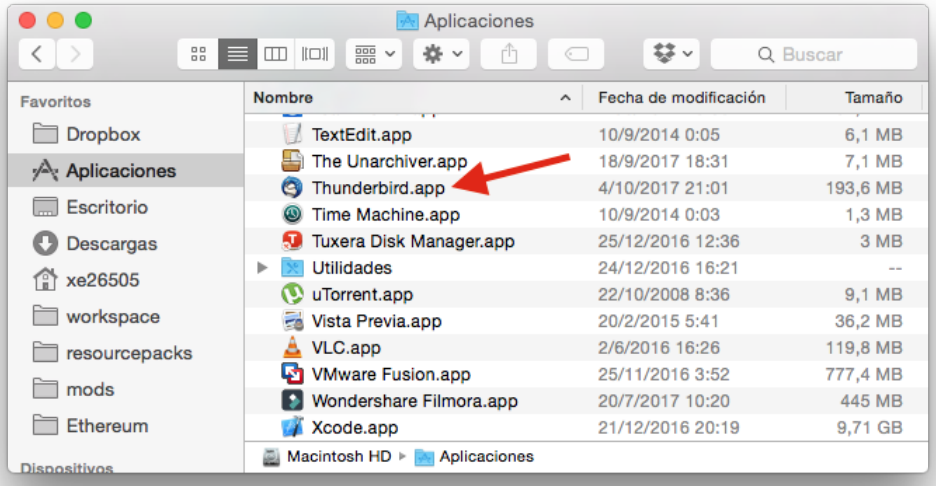


19. Una vez finalice la descarga, en la carpeta de Descargas aparecerá un archivo ejecutable llamado **Thunderbird 52.4.0.dmg**. Para instalarlo hay que hacer doble click en él:

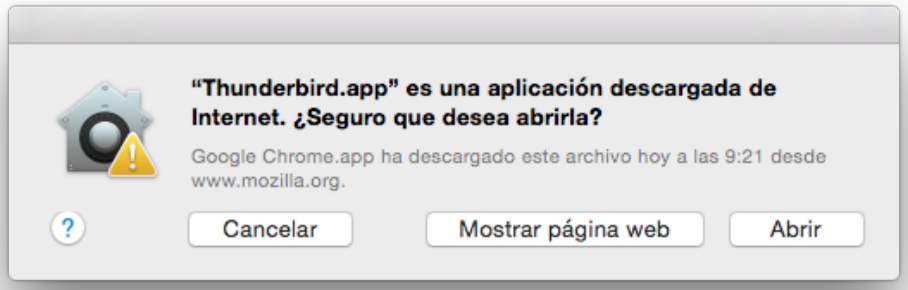


20. Se abrirá la siguiente ventana. Hay que arrastrar el icono “**Thunderbird.app**” dentro de la carpeta de “**Aplicaciones**”:

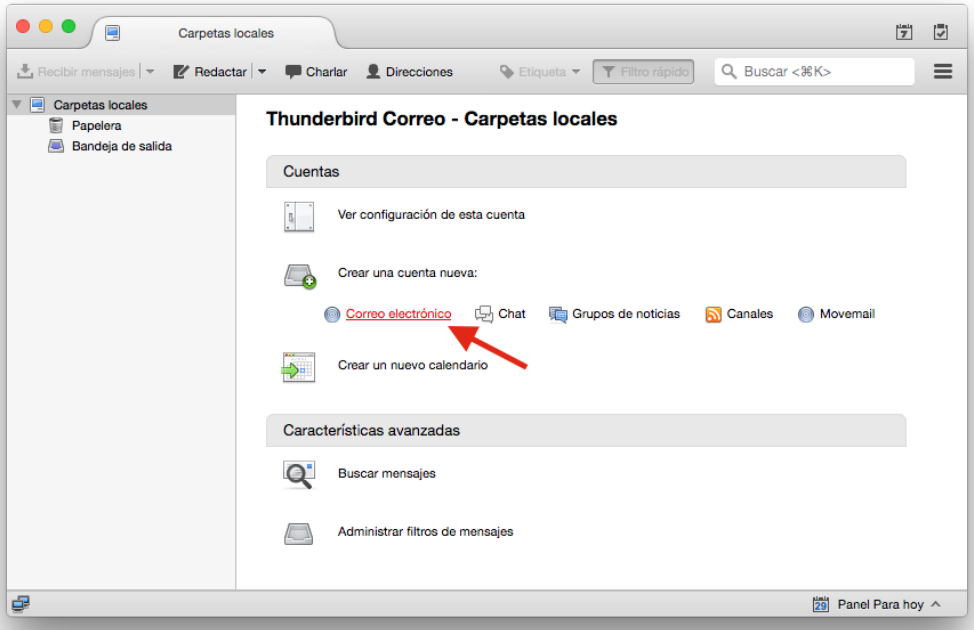
21. Una vez finalice la instalación hay que abrir la carpeta “**Aplicaciones**” y hacer doble click en “**Thunderbird.app**”:



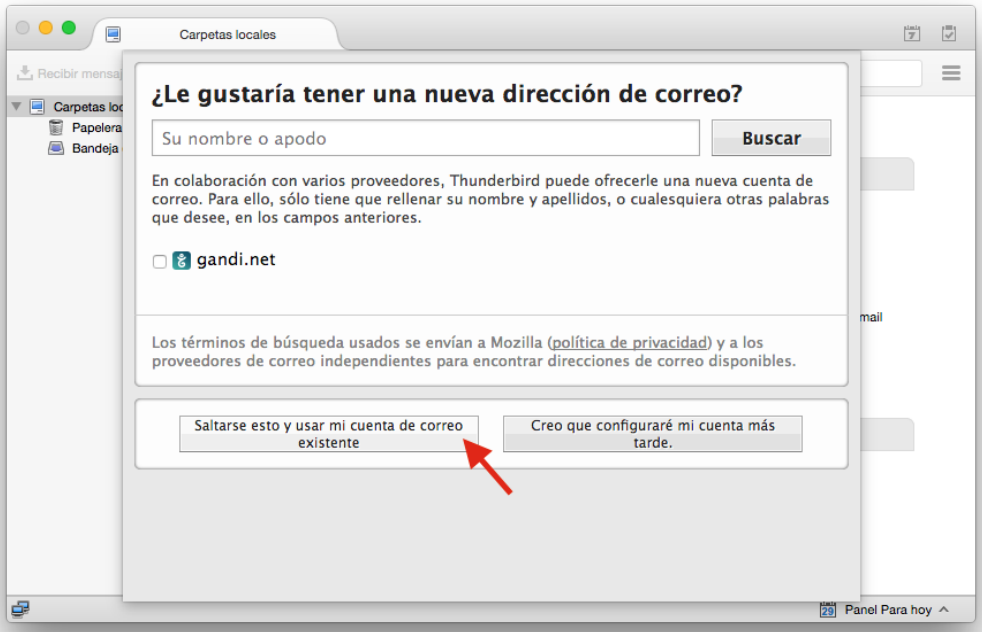
22. Al abrir Thunderbird por primera vez es posible que aparezca una ventana como esta, se pulsa el botón "**Abrir**":



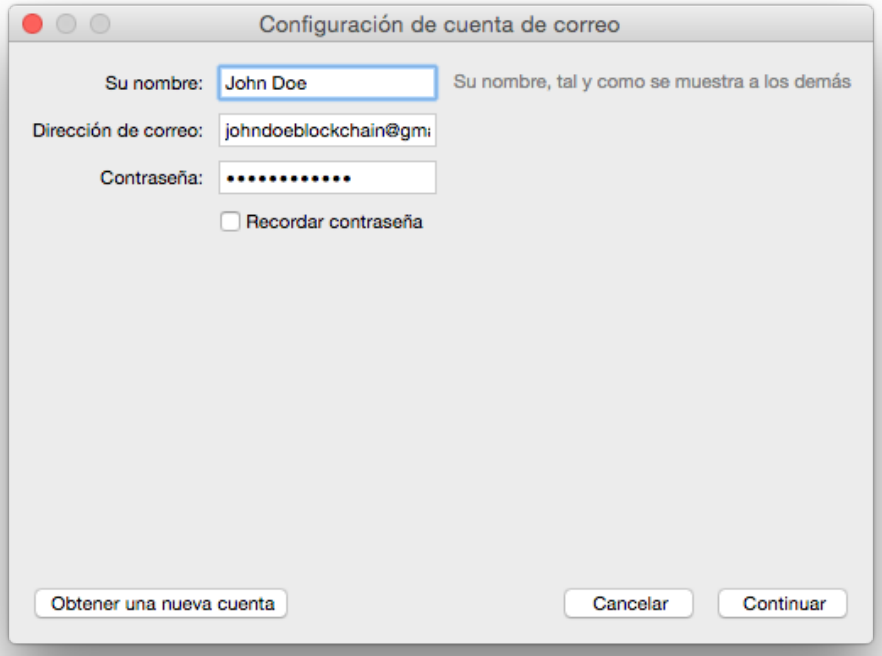
23. Lo primero que hay que hacer configurar la cuenta de correo existente, en este ejemplo se la cuenta johndoeblockchain@gmail.com. Para ello se ha de pulsar primero en la opción del menú de la izquierda "**Carpetas locales**", luego en la parte de "**Crear una cuenta nueva**" sobre la opción "**Correo electrónico**":



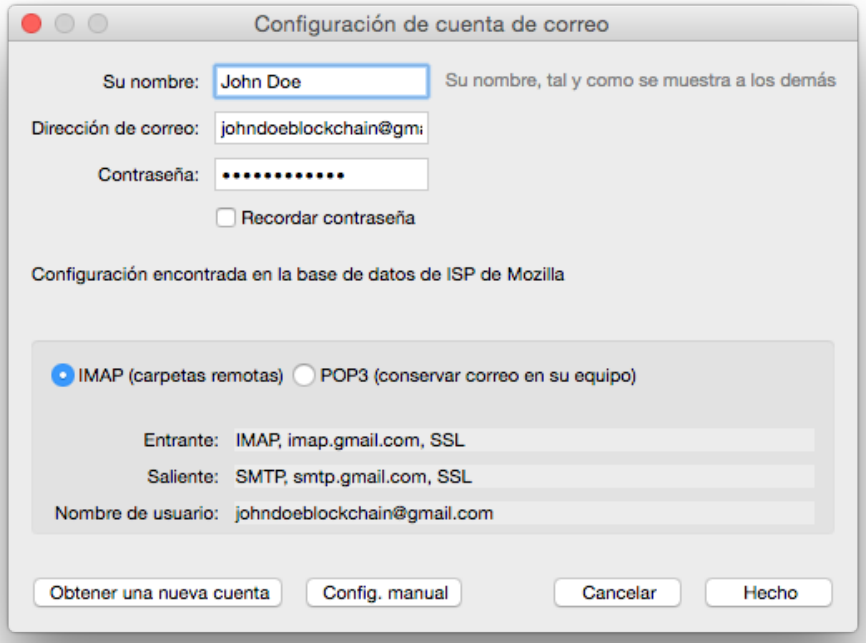
24. En esta nueva ventana se ha de desactivar el checkbox que dice “**gandi.net**” y se pulsa el botón “**Saltarse esto y usar mi cuenta de correo existente**”:



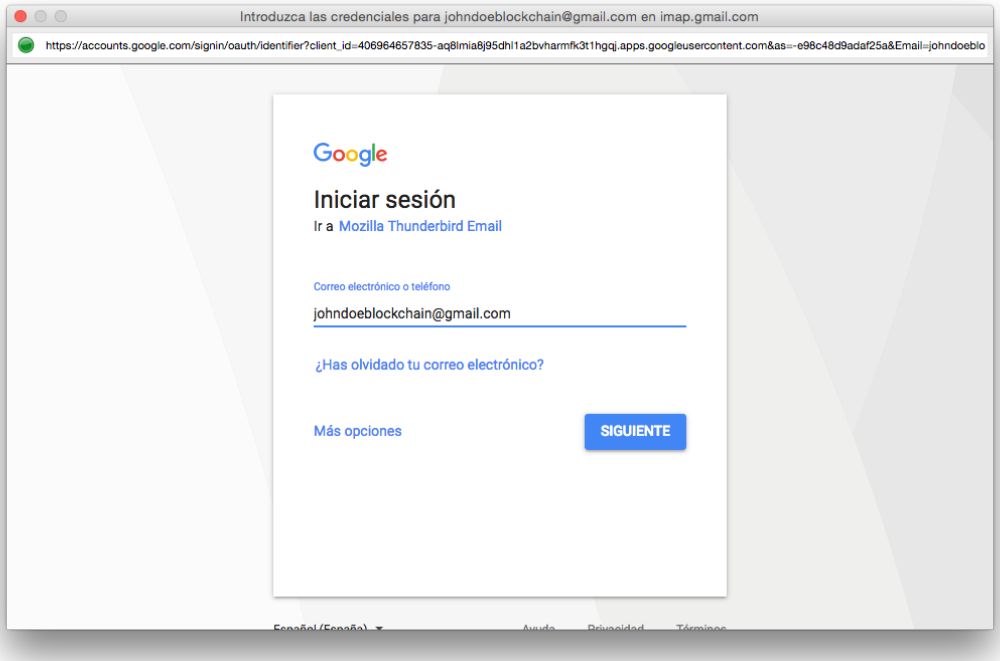
25. Se rellenan los campos nombre, dirección de correo, password y finalmente se desactiva la opción “**Recordar contraseña**”, esto último es una recomendación, se puede activar, pero es menos seguro. Finalmente se pulsa el botón “**Continuar**”:



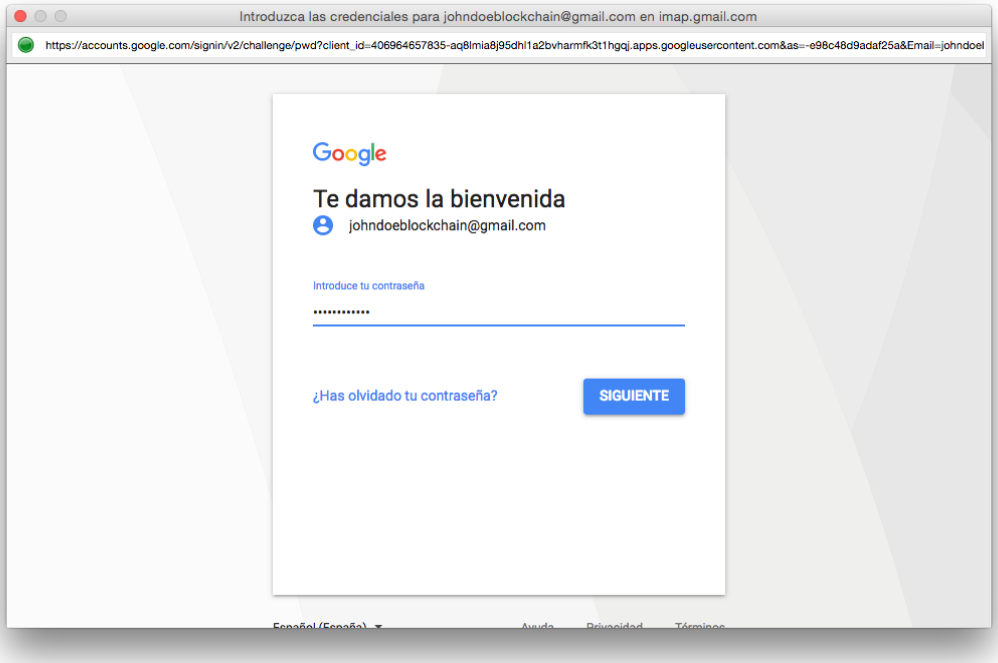
26. Se deja activada la opción “**IMAP (carpetas remotas)**” y se pulsa el botón “**Hecho**”:



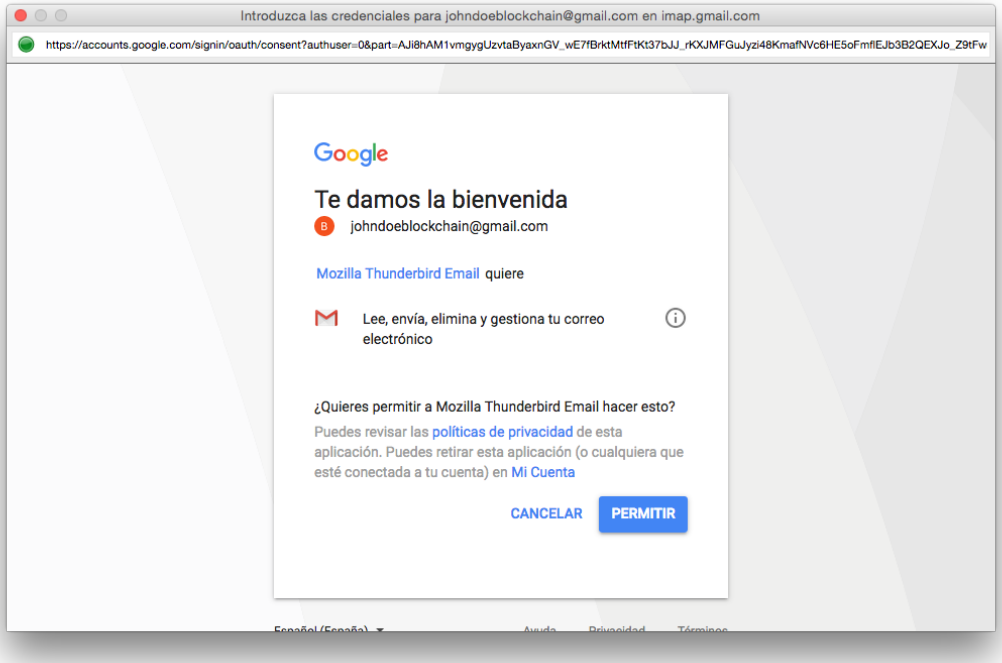
27. En el ejemplo se ha usado una cuenta de correo de Gmail, en este caso se abrirá una ventana de un navegador para introducir las credenciales de la cuenta de correo. Se pulsa el botón “**Siguiente**”:



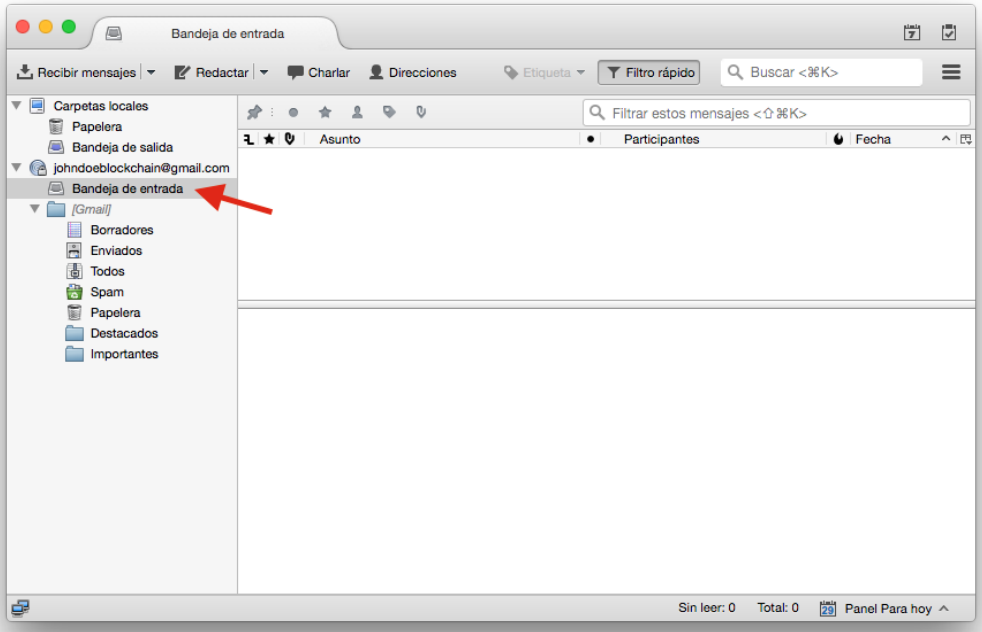
28. Se añade la password y se pulsa sobre el botón “**Siguiente**”:



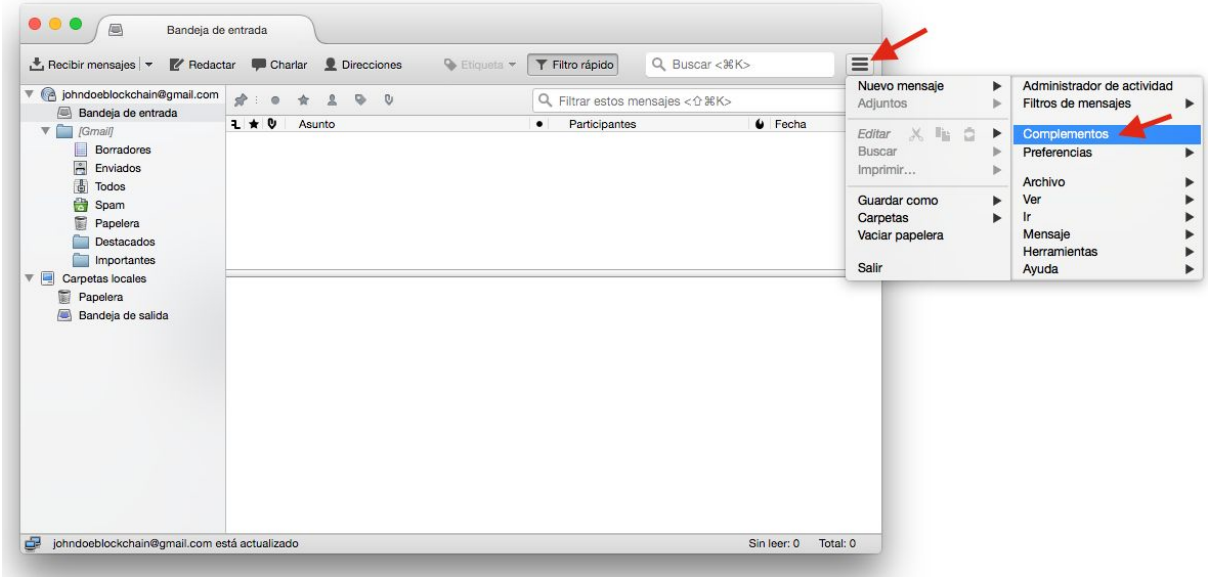
29. Se pulsa el botón “**Permitir**”:



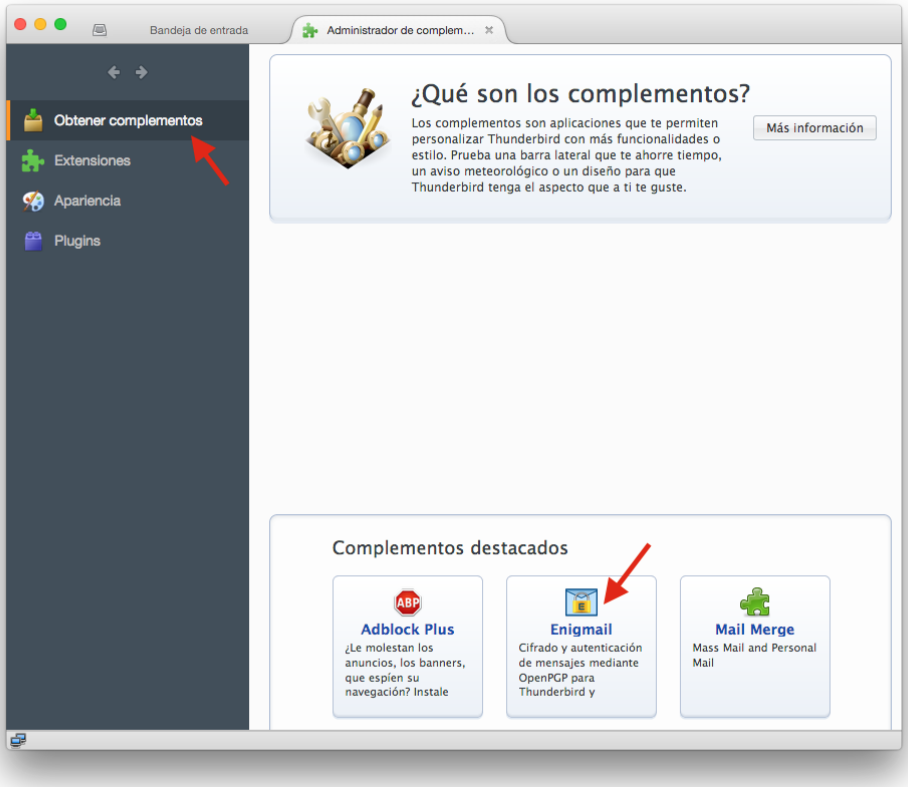
30. Ya estaría configurada la cuenta de correo johndoeblockchain@gmail.com en el cliente de correo Thunderbird. Se puede pinchar sobre la opción "**Bandeja de entrada**" para ver los correos recibidos:



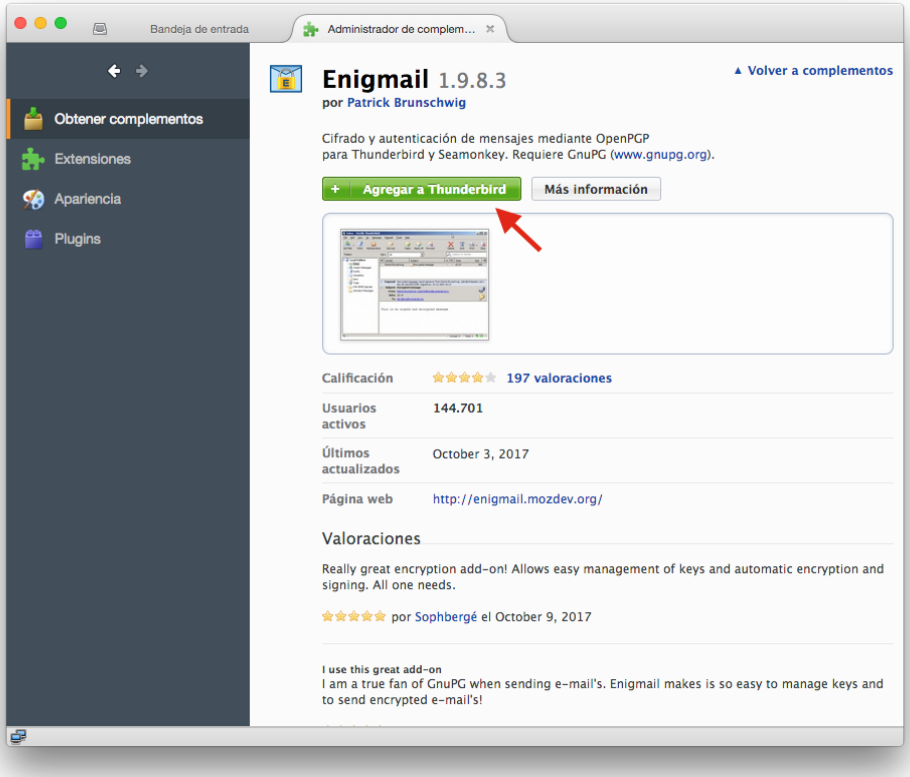
31. Ahora solo falta instalar **Enigmail**, se trata de un complemento de Thunderbird que permite acceder a las funciones de encriptación de GnuPG desde dentro de Thunderbird. Para ello, desde Thunderbird hay que pinchar en el botón que se muestra en la siguiente imagen y luego en la opción "**Complementos**":



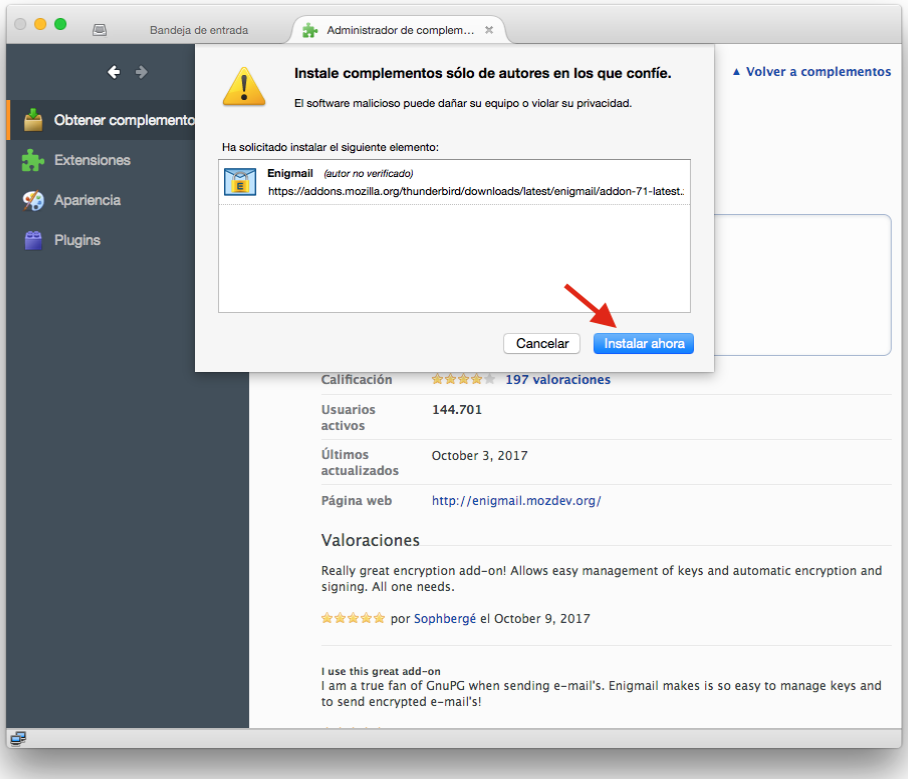
32. En “**Obtener complementos**”, más abajo aparece entre los complementos más destacados “**Enigmail**”:



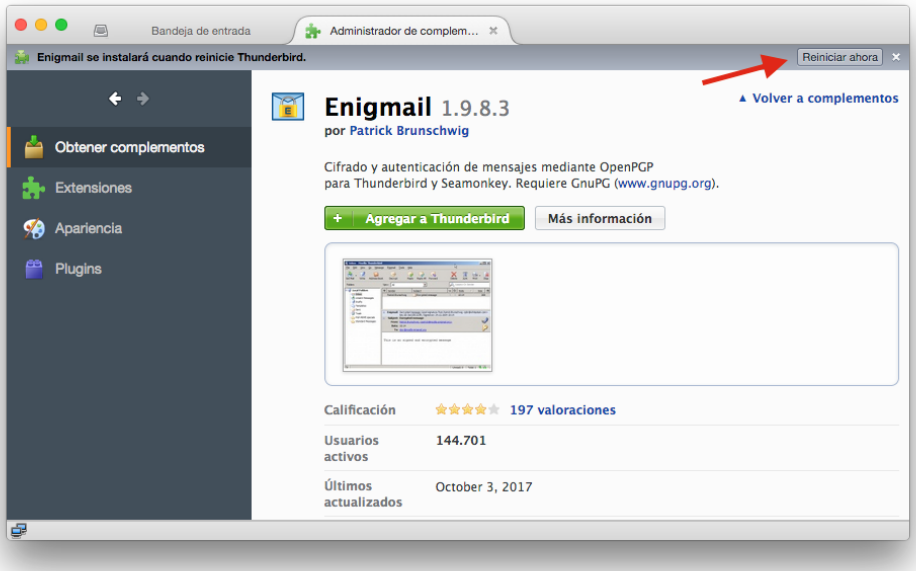
33. Pulsar el botón “**Agregar a Thunderbird**”:



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



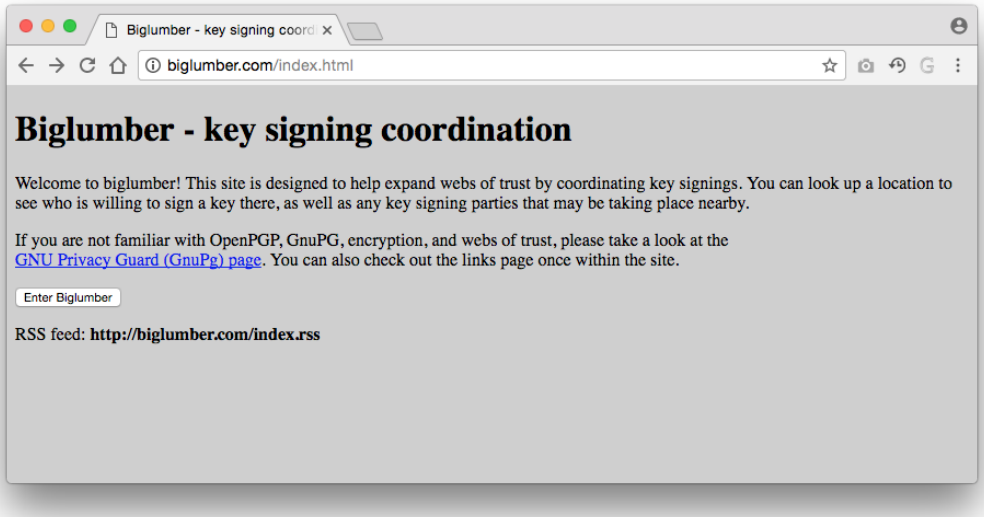
35. Pulsar el botón “**Reiniciar ahora**” que aparece en la parte superior derecha de Thunderbird:



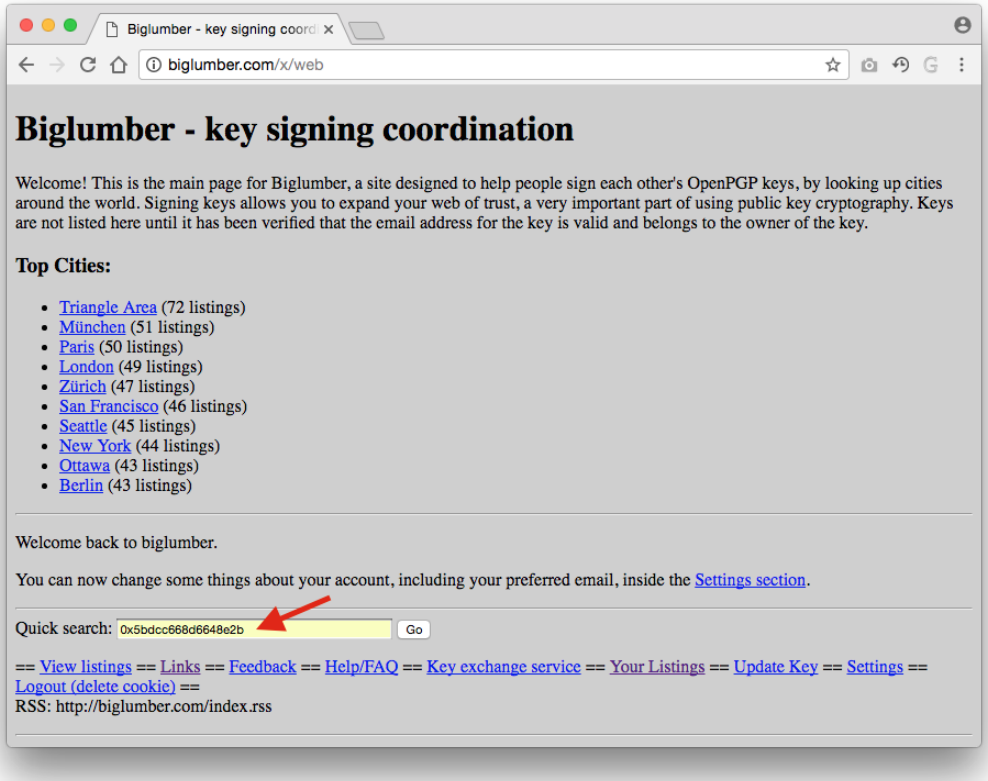
36. Antes de probar a mandar un mail cifrado a alguien primero debemos añadir la clave pública de ese “alguien” a GnuPG, para ello primero hay que ir a la siguiente URL:

http://www.biglumber.com

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

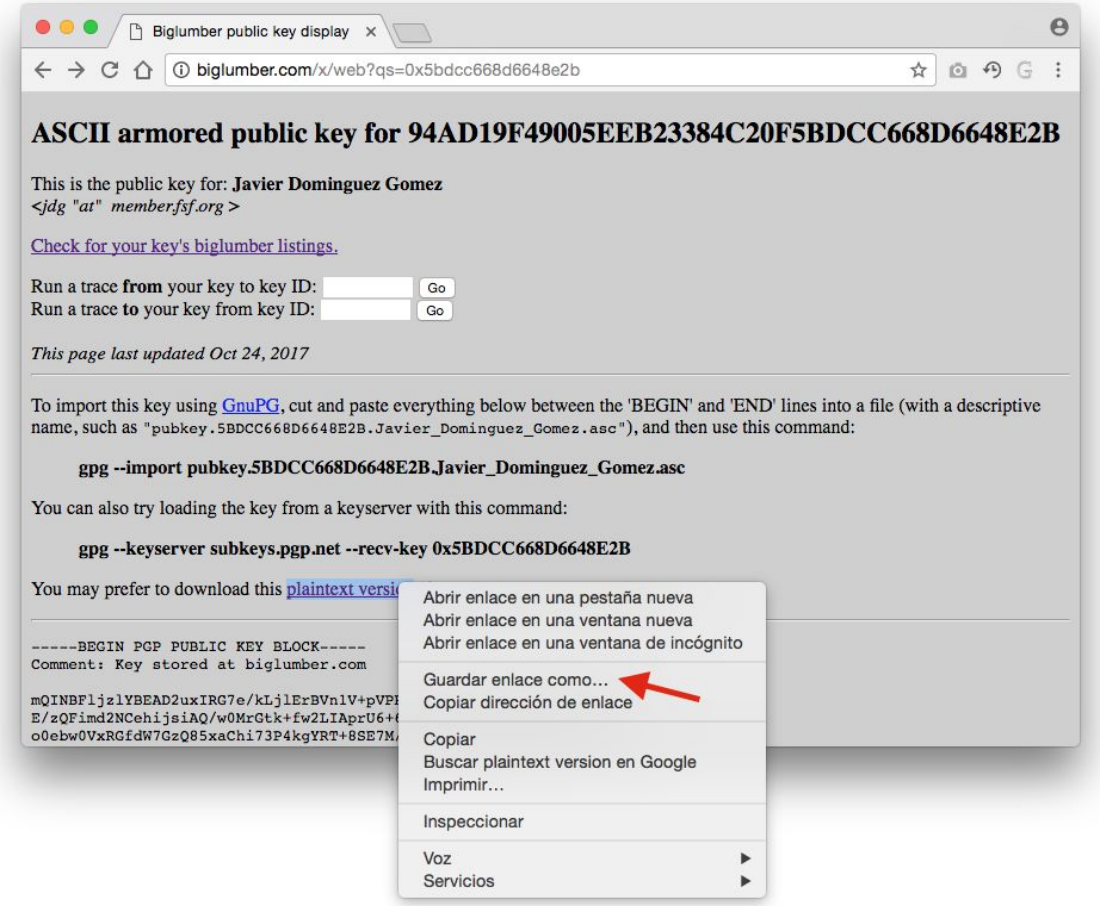


37. Una vez dentro buscar la clave pública, por ejemplo, de Javier Dominguez Gomez mediante la siguiente cadena hexadecimal: **0x5bdcc668d6648e2b**

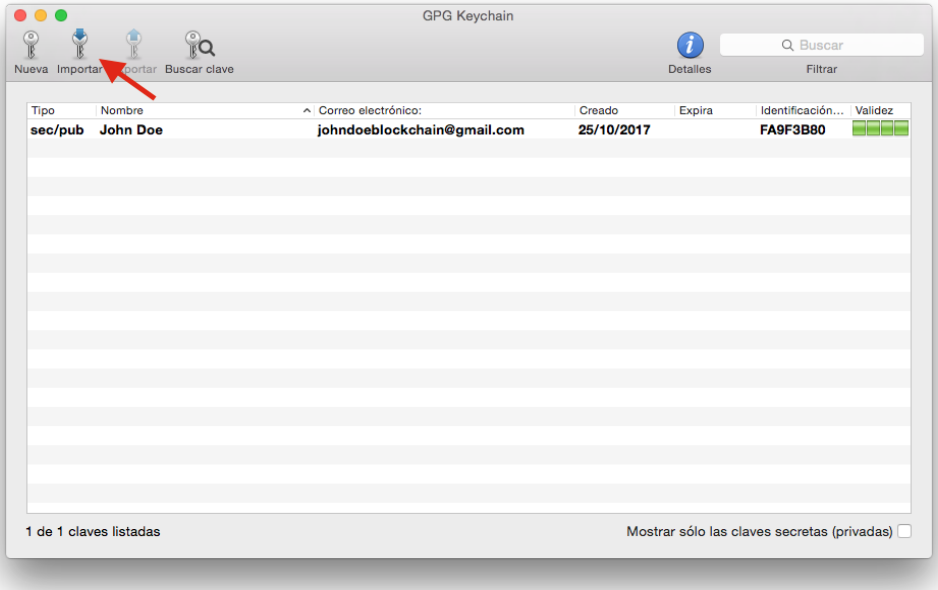


y pulsar el botón “**Go**”.

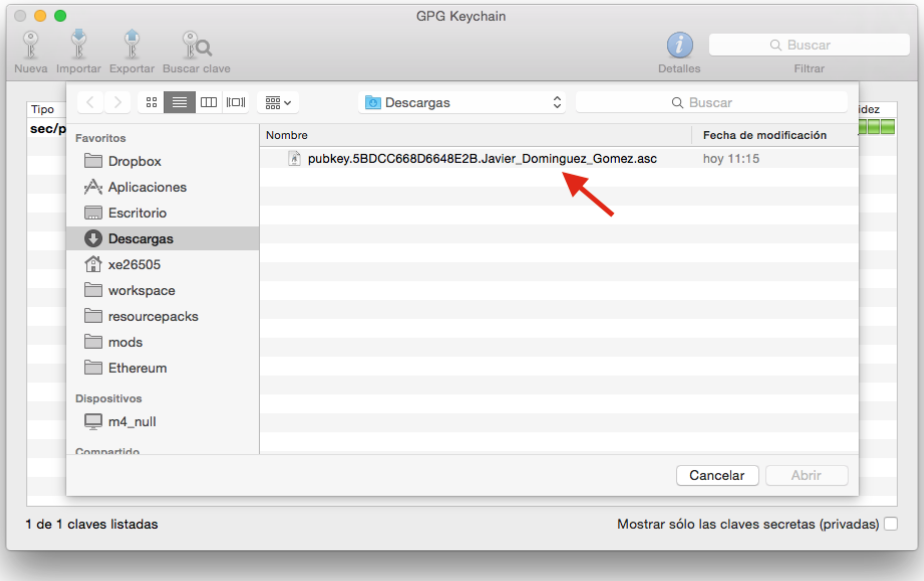
38. Descargar en archivo de texto plano la clave pública de Javier Domínguez Gómez, para ello hay que hacer click con el botón derecho del ratón sobre el link "**plaintext version**", seleccionar la opción "**Guardar enlace como…**" y guardarlo en alguna carpeta local, por ejemplo "**Descargas**".



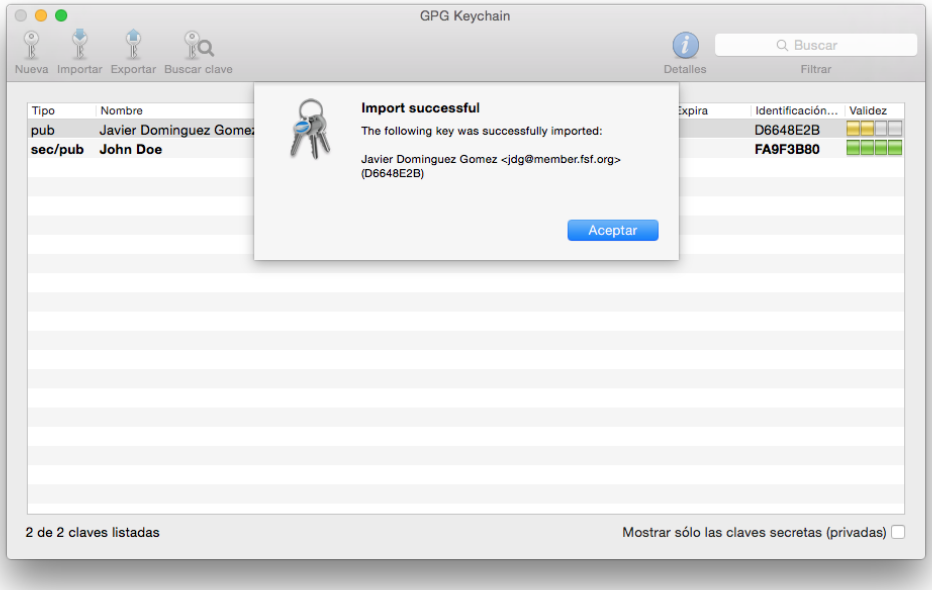
39. Una vez descargada la la clave pública hay que ir a la aplicación **GPG Keychain** de nuevo y pulsar el botón "**Importar**".



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

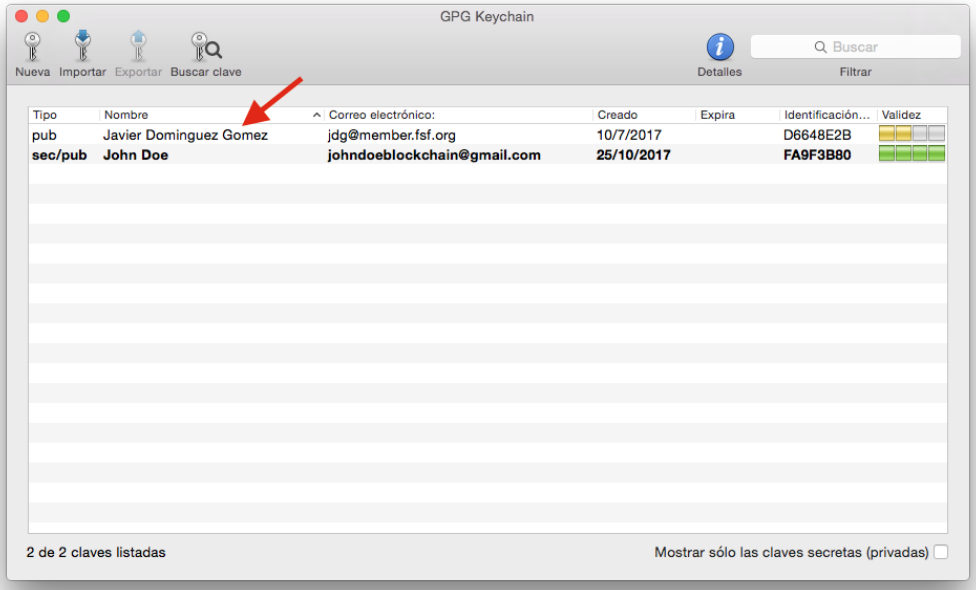


41. Se pulsa el botón "**Aceptar**":

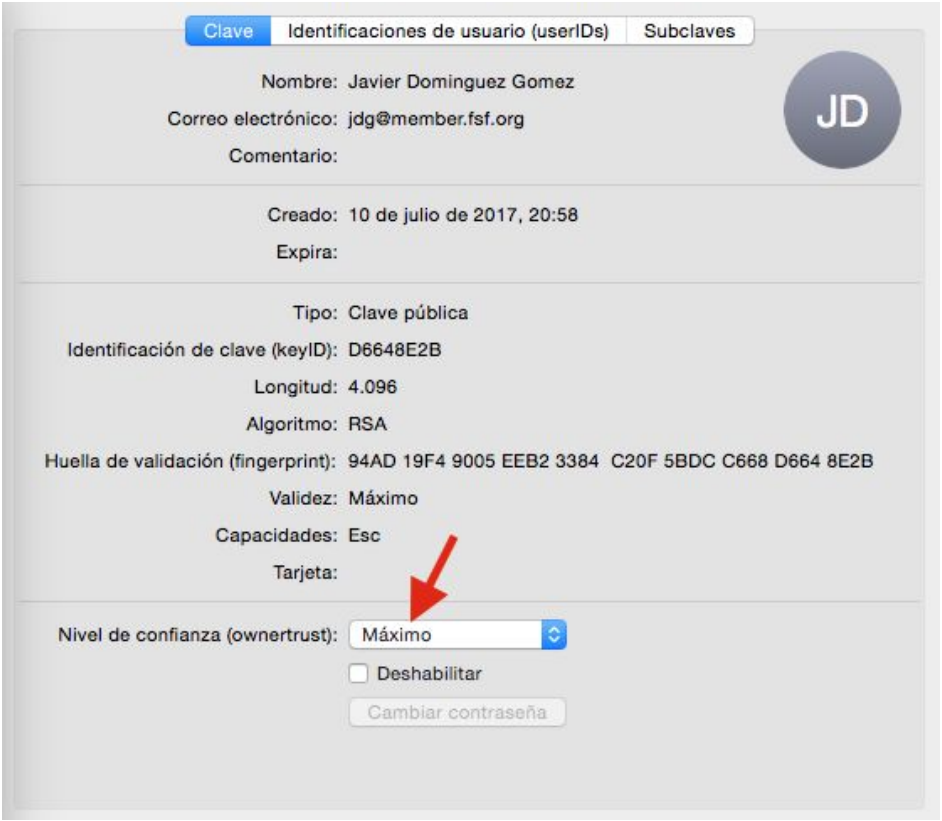


42. Una buena práctica es verificar previamente con el dueño de la clave pública que se quiere importar la huella digital o *fingerprint* del mismo, en este caso os la doy por aquí (la que viene en la cabecera de la imágen del punto 38, o sea "94AD19F49005EEB23384C20F5BDCC668D6648E2B"), o si queréis me lo podéis preguntar por Telegram (*@xe26505*), por twitter (*@ingenieriainv*) o en persona quedando conmigo en una *Key signing party* o cualquier otra circunstancia.

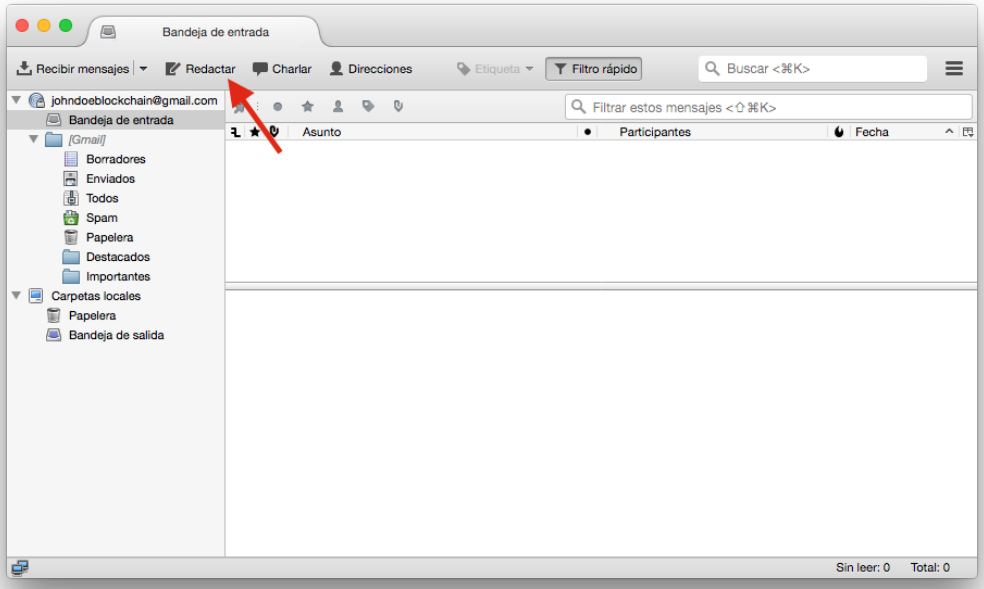
43. Una vez importada esta clave pública de ejemplo o cualquier otra, aparecerá en la lista de claves que se tienen almacenadas en la aplicación GnuPG, incluída la nuestra (sec/pub):



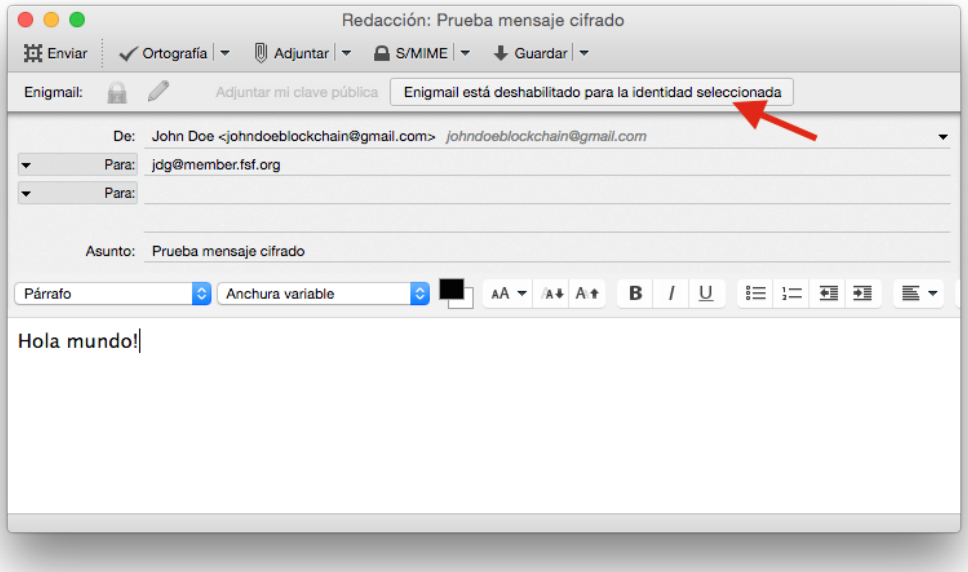
44. A esta nueva clave pública o identidad que se acaba de añadir a GnuPG hay que añadirle un nivel de confianza, para ello hay que hacer doble click sobre la clave y seleccionar "**Máximo**" del combo de la siguiente imagen:



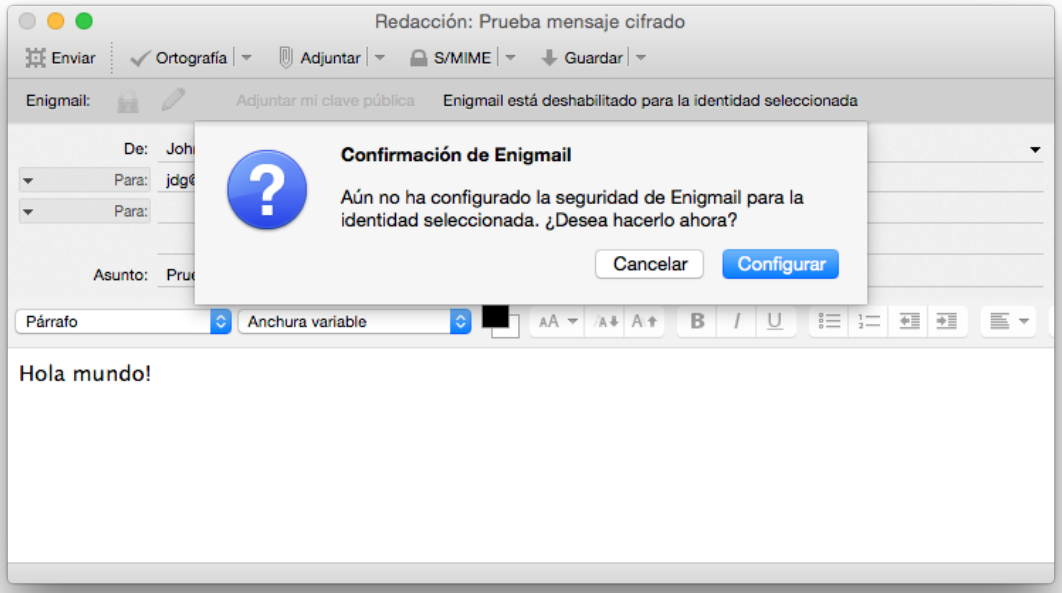
45. Ahora hay que probar a mandar un mail encriptado a la persona cuya clave pública se acaba de importar en GnuPG. Para ello hay que volver a Thunderbird y pulsar el botón “**Redactar**”:



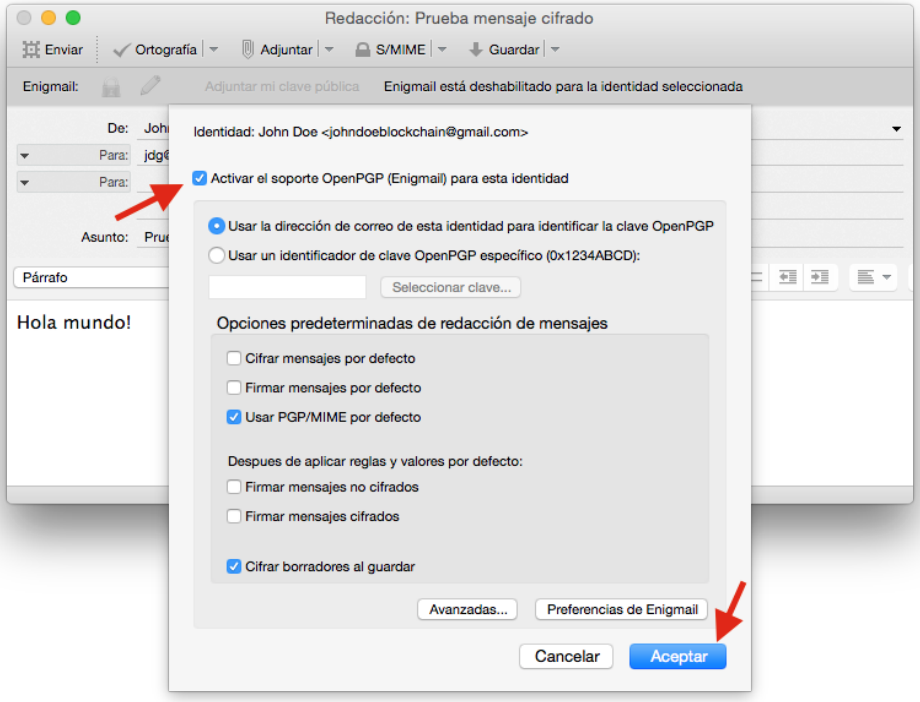
46. Hay que rellenar los campos “**Para:**”, “**Asunto:**” y hay que escribir un mensaje cualquiera. Antes de poder encriptar y firmar el mail es necesario la primera vez activar GnuPG para la identidad “*John Doe*” de Thunderbird. Para ello hay que hacer click sobre el botón “**Enigmail está deshabilitado para la identidad seleccionada**”:



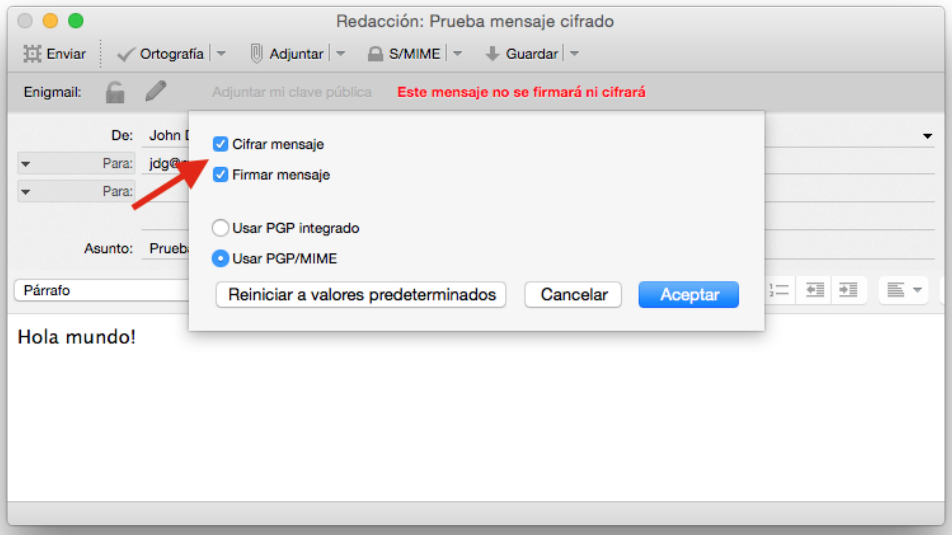
47. Pulsar el botón “**Configurar**”:



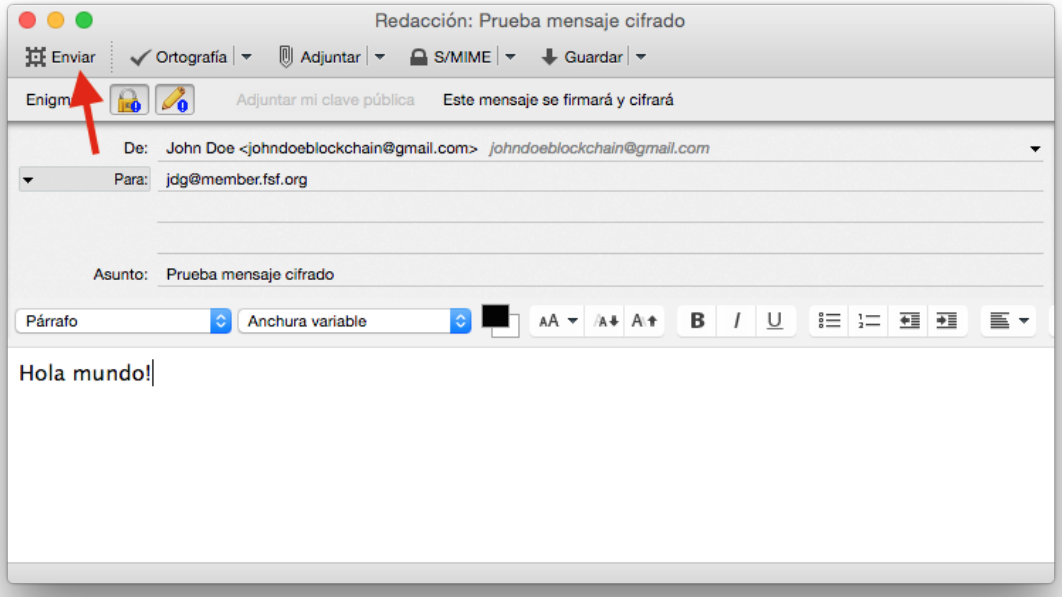
48. Se activa el checkbox que dice “**Activar el soporte OpenPGP (Enigmail) para esta identidad”** y se pulsa el botón “**Aceptar**:



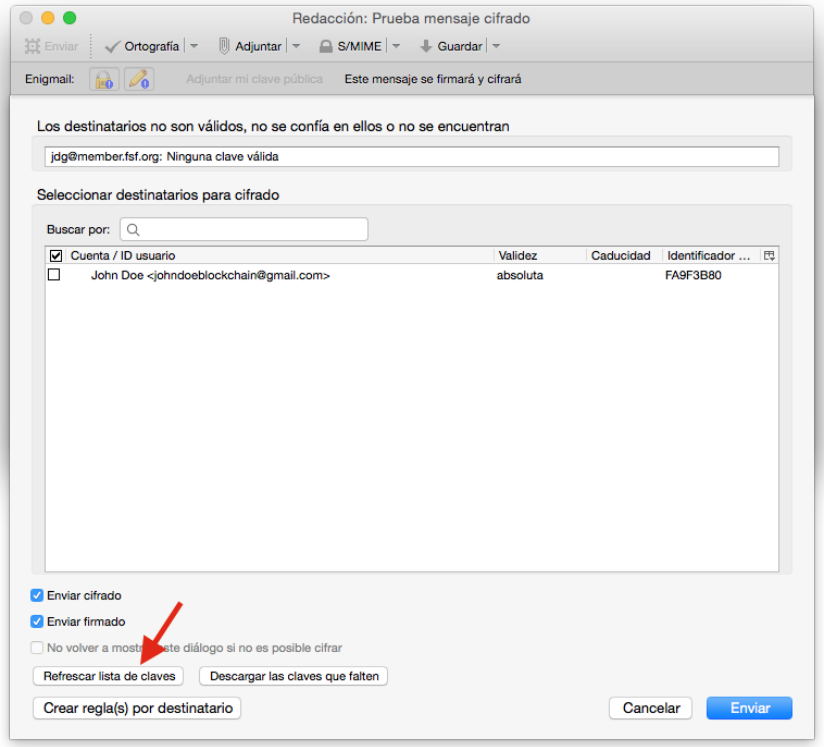
49. A continuación aparecerá la siguiente ventana, hay que activar los dos checkboxes donde pone "**Cifrar mensaje**" y "**Firmar mensaje**". Finalmente se pulsa el botón "**Aceptar**":



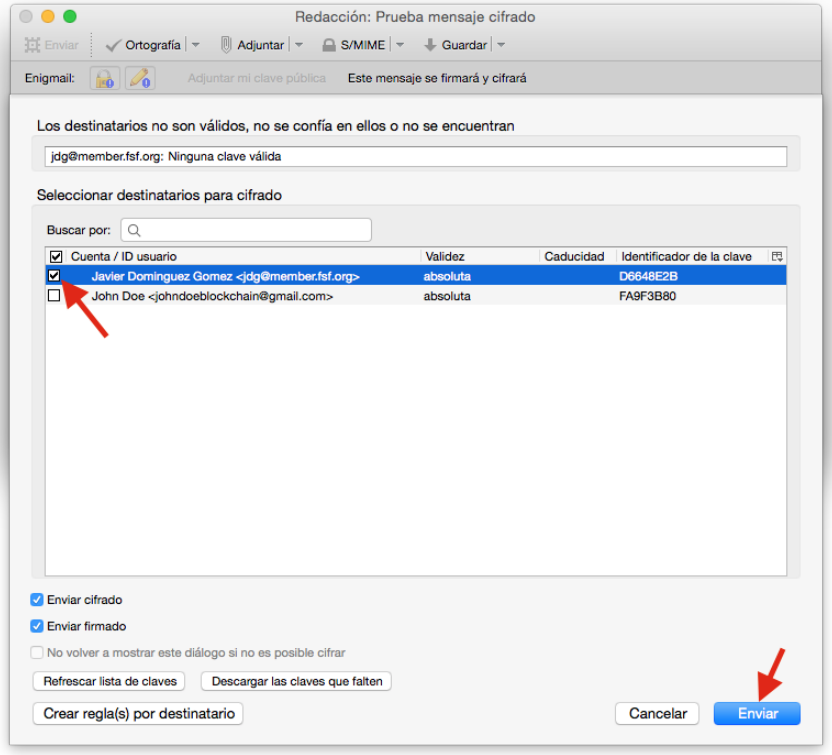
50. Se pulsa el botón "**Enviar**":



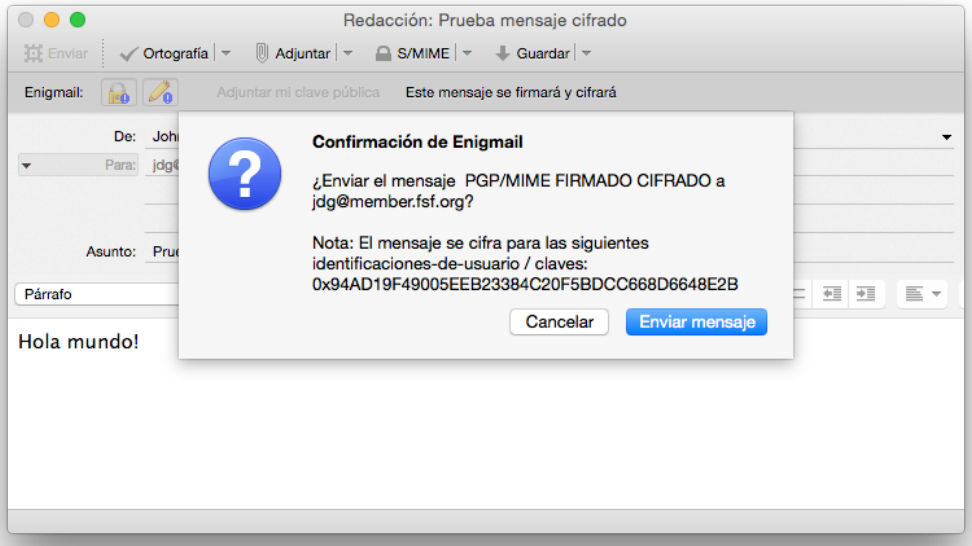
51. Si al darle al botón de “**Enviar**” aparece la siguiente pantalla hay que darle al botón “**Refrescar lista de claves**” y pulsar el botón “**Enviar**”:



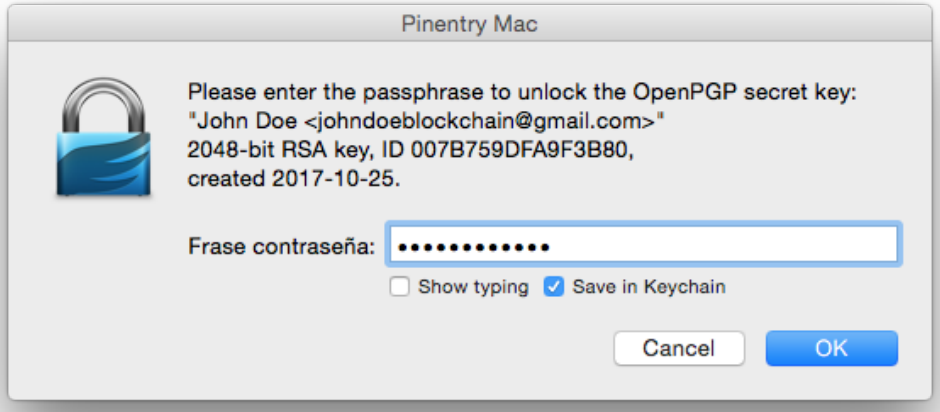
52. Al refrescar la lista de claves aparecerá la última que se ha añadido, y que coincide con la del destinatario al que se le quiere mandar un mail cifrado. Se selecciona ese destinatario y se pulsa el botón “**Enviar**”:



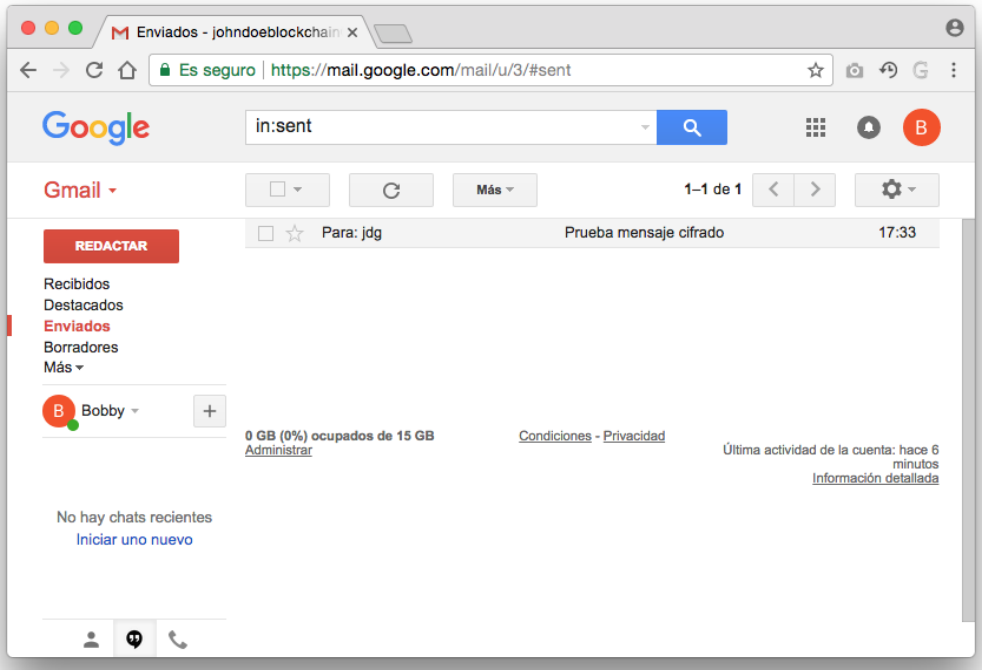
53. Pulsar el botón “**Enviar mensaje**”:



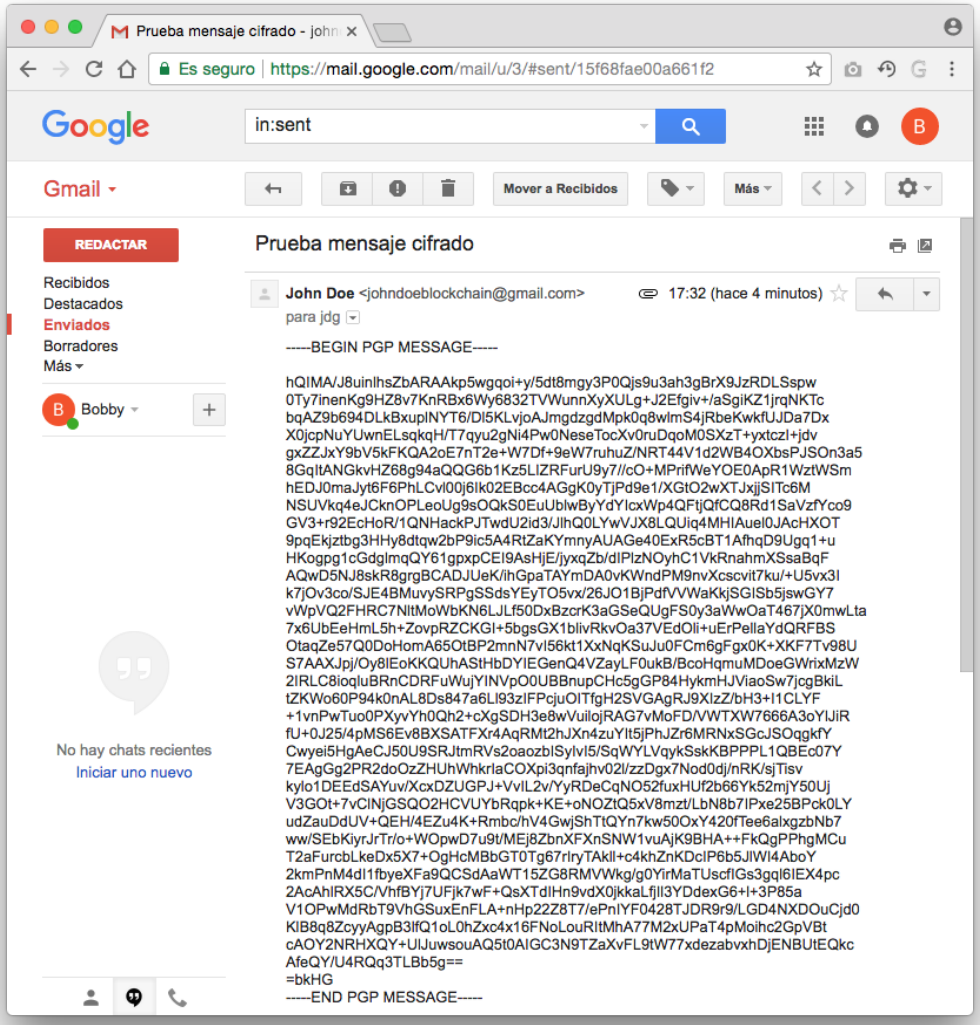
54. Aparecerá la siguiente ventana pidiendo introducir la password de la clave privada que se seleccionó en el paso 12 de esta guía, se introduce, se pulsa el botón “**OK**” y el mail se enviará cifrado y firmado:



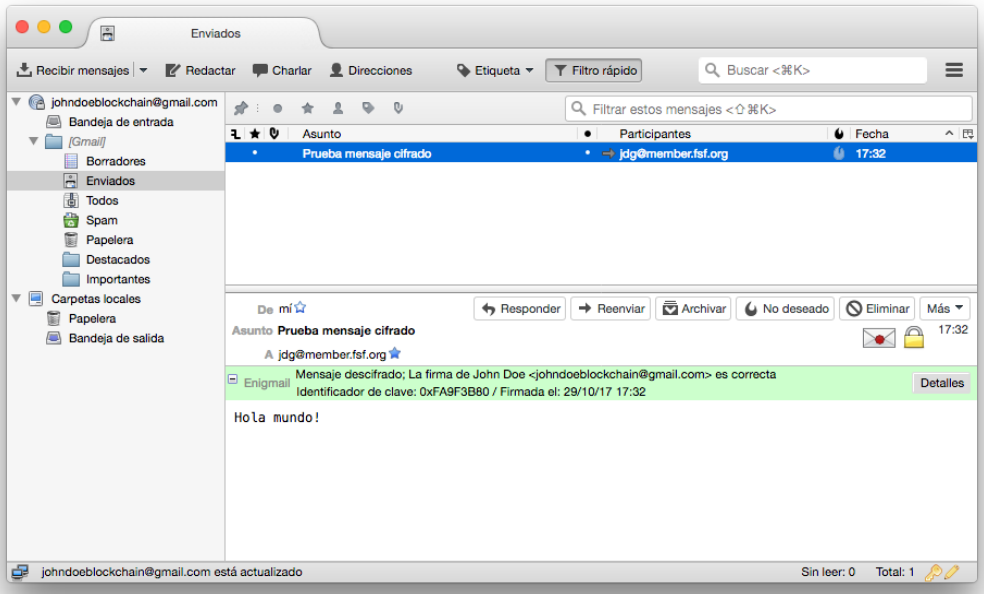
55. Una manera de ver cómo se ha enviado este mail cifrado desde la cuenta de Gmail johndoeblockchain@gmail.com a la cuenta de mail de Javier Domínguez Gómez jdg@member.fsf.org es yendo a la página de Gmail, hacer login, pinchar en elementos enviados y luego en el mail enviado.



56. 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:


Prueba mensaje cifrado - john
Es seguro | https://mail.google.com/mail/u/3/#sent/15f68fae00a661f2
Google
in:sent
Gmail
Mover a Recibidos
Más
REDACTAR
Recibidos
Destacados
Enviados
Borradores
Más
Bobby
No hay chats recientes
Iniciar uno nuevo
Prueba mensaje cifrado
John Doe <johndoeblockchain@gmail.com>
17:32 (hace 4 minutos)
para jdg
-----BEGIN PGP MESSAGE-----
hQIMA/J8uinlhsZbARAAkp5wgqoi+y/5dt8mgy3P0Qjs9u3ah3gBrX9JzRDLSspw
0Ty7inenKg9HZ8v7KnRBx6Wy6832TVWunnXyXULg+J2Efgiv+/aSgiKZ1jrqNKTc
bqAZ9b694DLkBxuplNYT6/Dl5KLvjoAJmgdzgdMpk0q8wlmS4jRbeKwkfUJDa7Dx
X0jcpNuYUwnELsqkqH/T7qyu2gNi4Pw0NeseTocXv0ruDqoM0SXzT+yxtczI+jdv
gxZZJxY9bV5kFKQA2oE7nT2e+W7Df+9eW7ruhuZ/NRT44V1d2WB4OXbsPJSOn3a5
8GqItANGkvHZ68g94aQQG6b1Kz5LlZRFurU9y7//cO+MPrifWeYOE0ApR1WztWSm
hEDJ0maJyt6F6PhLCvl00j6Ik02EBcc4AGgK0yTjPd9e1/XGtO2wXTJxjjSlTc6M
NSUVkq4eJCknOPLeoUg9sOQkS0EuUblwByYdYlcxWp4QFtjQfCQ8Rd1SaVzfYco9
GV3+r92EcHoR/1QNHackPJTwdU2id3/JlhQ0LYwVJX8LQUiq4MHIAuel0JAcHXOT
9pqEkjztbg3HHy8dtqw2bP9ic5A4RtZaKYmnyAUAGe40ExR5cBT1AfhqD9Ugq1+u
HKogpg1cGdglmqQY61gpxpCEl9AsHjE/jyxqZb/dlPlzNOyhC1VkRnahmXSsaBqF
AQwD5NJ8skR8grgBCADJUeK/ihGpaTAYmDA0vKWndPM9nvXcscvit7ku/+U5vx3l
k7jOv3co/SJE4BMuvySRPgSSdsYEyTO5vx/26JO1BjPdfVVWaKkjSGlSb5jswGY7
vWpVQ2FHRC7NltMoWbKN6LJLf50DxBzcrK3aGSeQUgFS0y3aWwOaT467jX0mwLta
7x6UbEeHmL5h+ZovpRZCKGl+5bgsGX1blivRkvOa37VEdOli+uErPellaYdQRFBS
OtaqZe57Q0DoHomA65OtBP2mnN7vl56kt1XxNqKSuJu0FCm6gFgx0K+XKF7Tv98U
S7AAXJpj/Oy8lEoKKQUhAStHbDYIEGenQ4VZayLF0ukB/BcoHqmuMDoeGWrixMzW
2IRLC8ioqluBRnCDRFuWujYINVpO0UBBnupCHc5gGP84HykmHJViaoSw7jcgBkiL
tZKWo60P94k0nAL8Ds847a6LI93zIFPcjuOlTfgH2SVGAgRJ9XIzZ/bH3+I1CLYF
+1vnPwTuo0PXyvYh0Qh2+cXgSDH3e8wVuilojRAG7vMoFD/VWTXW7666A3oYlJiR
fU+0J25/4pMS6Ev8BXSATFXr4AqRMt2hJXn4zuYlt5jPhJZr6MRNxSGcJSOqgkfY
Cwyei5HgAeCJ50U9SRJtmRVs2oaozbISylvI5/SqWYLVqykSskKBPPPL1QBEc07Y
7EAgGg2PR2doOzZHUhWhkrIaCOXpi3qnfajhv02l/zzDgx7Nod0dj/nRK/sjTisv
kylo1DEEdSAYuv/XcxDZUGPJ+VvIL2v/YyRDeCqNO52fuxHUf2b66Yk52mjY50Uj
V3GOt+7vClNjGSQO2HCVUYbRqpk+KE+oNOZtQ5xV8mzt/LbN8b7IPxe25BPck0LY
udZauDdUV+QEH/4EZu4K+Rmbc/hV4GwjShTtQYn7kw50OxY420fTee6alxgzbNb7
ww/SEbKiyrJrTr/o+WOpwD7u9t/MEj8ZbnXFXnSNW1vuAjK9BHA++FkQgPPhgMCu
T2aFurcbLkeDx5X7+OgHcMBbGT0Tg67rlryTAkll+c4khZnKDclP6b5JlWl4AboY
2kmPnM4dl1fbyeXFa9QCSdAaWT15ZG8RMVWkg/g0YirMaTUscfIGs3gql6lEX4pc
2AcAhlRX5C/VhfBYj7UFjk7wF+QsXTdlHn9vdX0jkkaLfjll3YDdexG6+l+3P85a
V1OPwMdRbT9VhGSuxEnFLA+nHp22Z8T7/ePnlYF0428TJDR9r9/LGD4NXDOuCjd0
KlB8q8ZcyyAgpB3lfQ1oL0hZxc4x16FNoLouRltMhA77M2xUPaT4pMoihc2GpVBt
cAOY2NRHXQY+UlJuwsouAQ5t0AlGC3N9TZaXvFL9tW77xdezabvxhDjENBUtEQkc
AfeQY/U4RQq3TLBb5g==
=bkHG
-----END PGP MESSAGE-----

57. Sin embargo, si se consulta la carpeta “**Enviados**” en Thunderbird y se selecciona el mail que se ha enviado encriptado, y aparecerá el mensaje en texto claro:



58. 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.