

Criptografía y seguridad 2022

Firma Digital

Firma digital de correos electrónicos

Para poder utilizar firma digital en correos electrónicos es necesario contar con un cliente de correos como Thunderbird

Ref: <https://www.howtogeek.com/706402/how-to-use-openpgp-encryption-for-emails-in-thunderbird/>

Configurar Thunderbird con el correo de la universidad

Account Setup - Mozilla Thunderbird

Home Account Setup x

Your full name
Javier JORGE

Email address
javier.jorge@unc.edu.ar

Password
.....

☒ Remember password

Configuration found in Mozilla ISP database.

Available configurations

☒ **IMAP**
Keep your folders and emails synced on your server
Incoming IMAP SSL/TLS
imap.gmail.com
Outgoing SMTP SSL/TLS
smtp.gmail.com
Username
javier.jorge@unc.edu.ar

☐ **POP3**
Keep your folders and emails on your computer

Not sure what to select?
[Setup documentation](#) - [Support forum](#) - [Privacy policy](#)

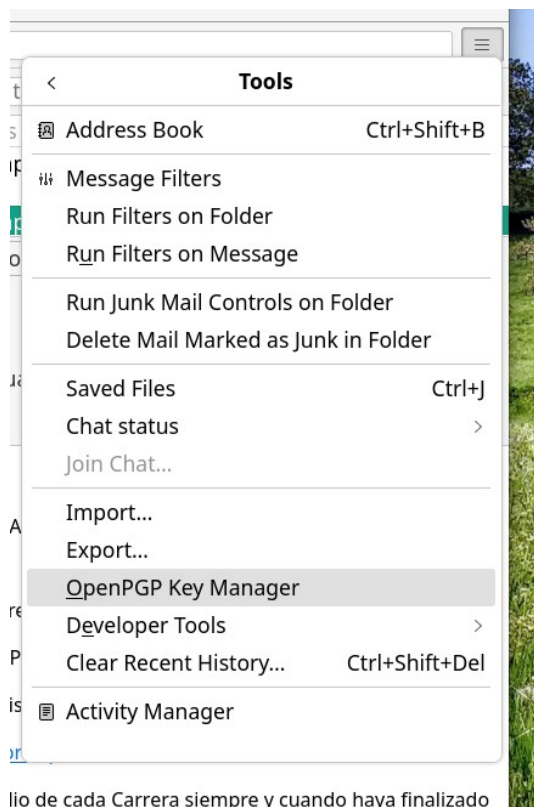
[Configure manually](#) Cancel Done

(en) <https://support.mozilla.org/products/thunderbird/emails-thunderbird/set-up-email-thunderbird>

Una vez configurado el cliente con el correo comenzará la descarga de los emails.

Generar el par de claves

Para generar el par de claves es necesario ir al menú que se encuentra en el vértice superior derecho



lio de cada Carrera siempre y cuando haya finalizado

Elegir la opción generar clave OpenPgp

Add a Personal OpenPGP Key for javier.jorge@unc.edu.ar ✕

Generate OpenPGP Key

Identity Javier JORGE <javier.jorge@unc.edu.ar> - javier.jorge@unc.edu.ar ▼

Key expiry
Define the expiration time of your newly generated key. You can later control the date to extend it if necessary.

☒ Key expires in ▼

☐ Key does not expire

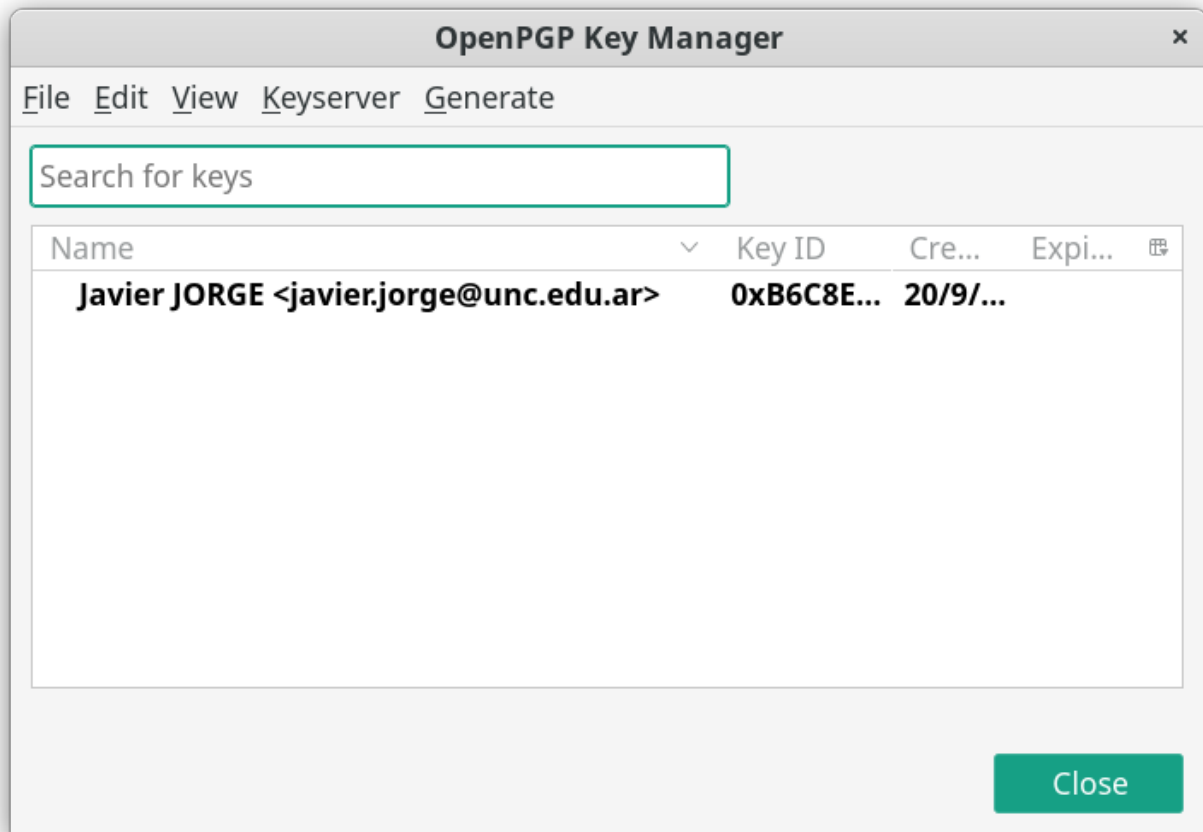
Advanced settings
Control the advanced settings of your OpenPGP Key.

Key type: RSA ▼

Key size: 3072 ▼

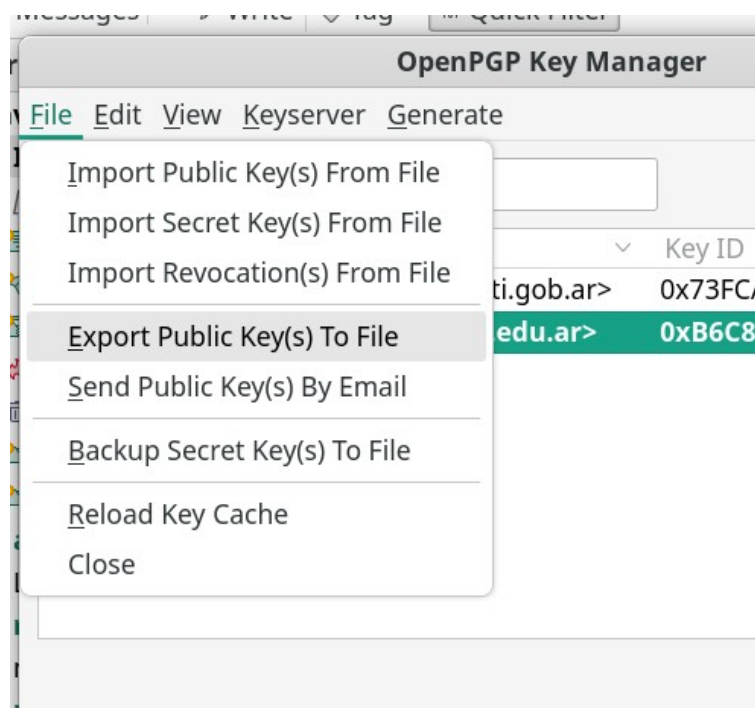
Go back Cancel Generate key

Debería verse así



Exportar la clave para publicarla en servidores de referencia

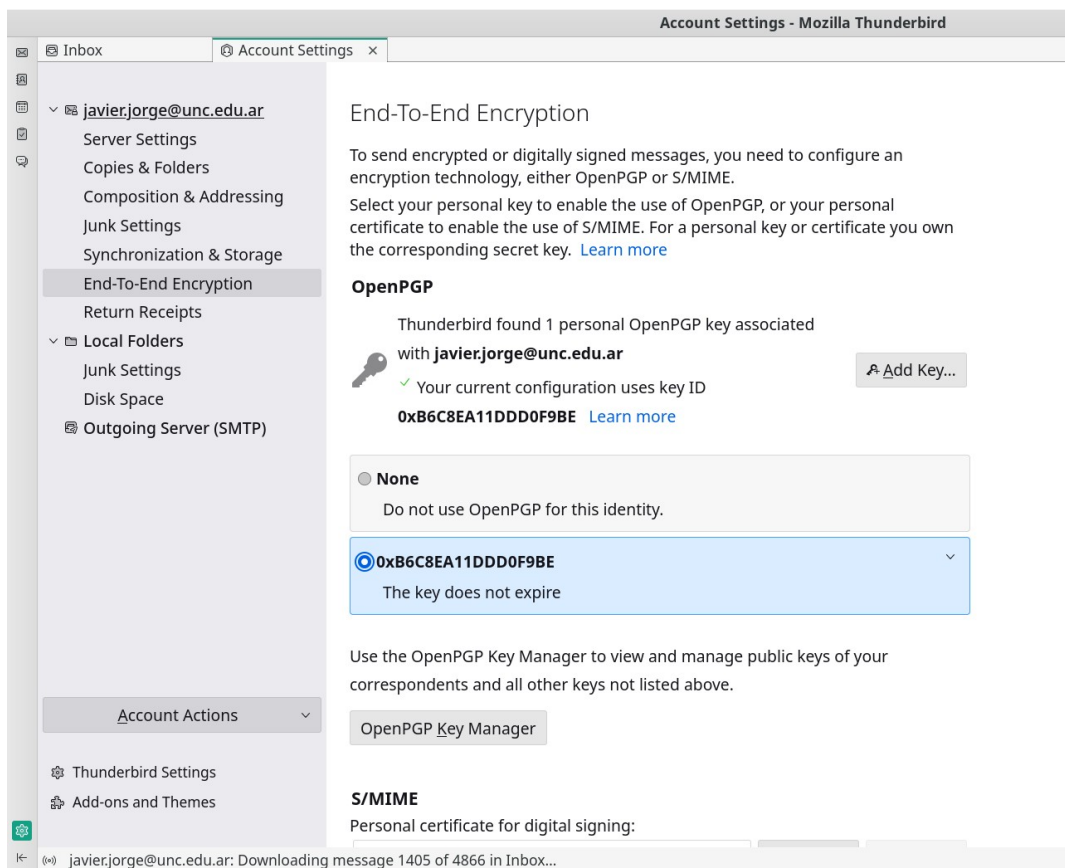
Una forma de intercambiar claves públicas es mediante el uso de servidores públicos de registro voluntario. Primero se exporta la clave a un archivo y luego se lo sube al sitio web.



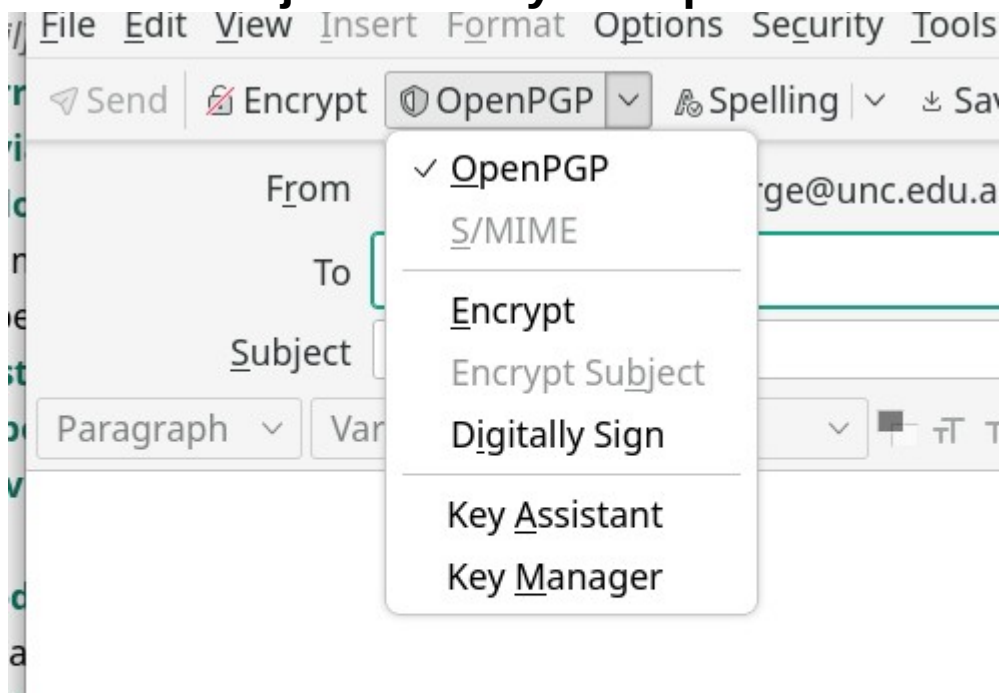
Subir el archivo al sitio <https://keys.openpgp.org/> y seguir los pasos para validar el correo y la clave

Configurar la cuenta para utilizar la clave generada

Hacer clic derecho sobre la dirección de correo y seleccionar la opción configuración. En la sección de encriptación de extremo a extremo seleccionar la clave generada para usarla por defecto en esta cuenta.



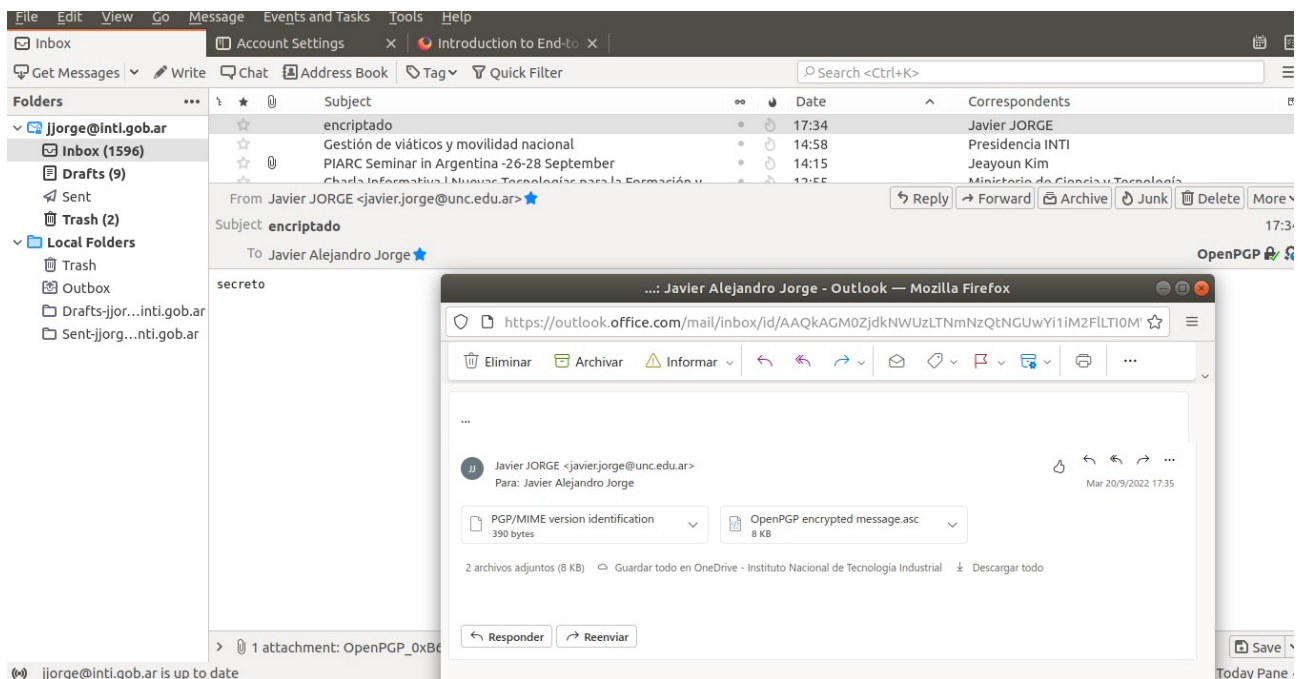
Enviar un mensaje firmado y encriptado



Primero es necesario compartir las claves. Por lo que solo podremos enviar un correo firmado por nosotros mismos. Se sugiere además agregar como adjunto la clave pública del remitente.

Cuando contemos con la clave pública del destinatario podremos enviar un correo encriptado.

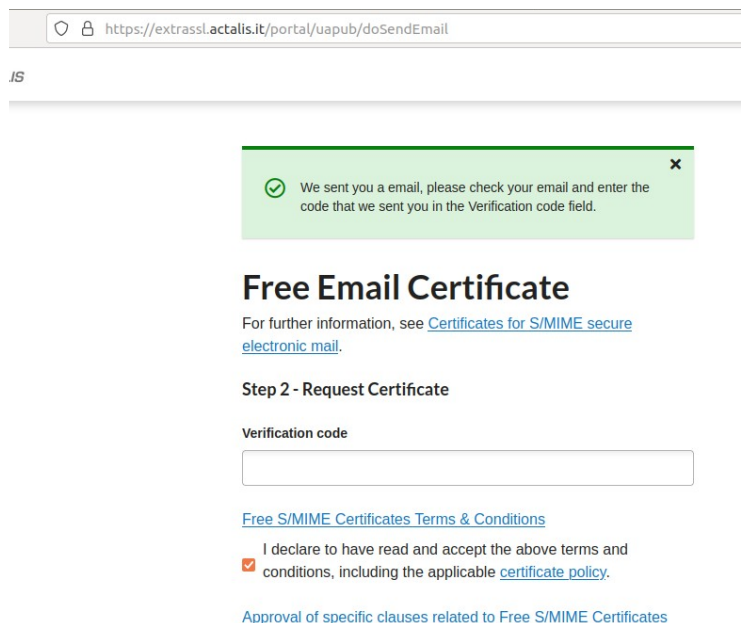
Al visualizar el correo desde el cliente web no podremos ver el contenido del mensaje. Solo en el cliente de correos podremos verlo.



Firma digital provista por terceros

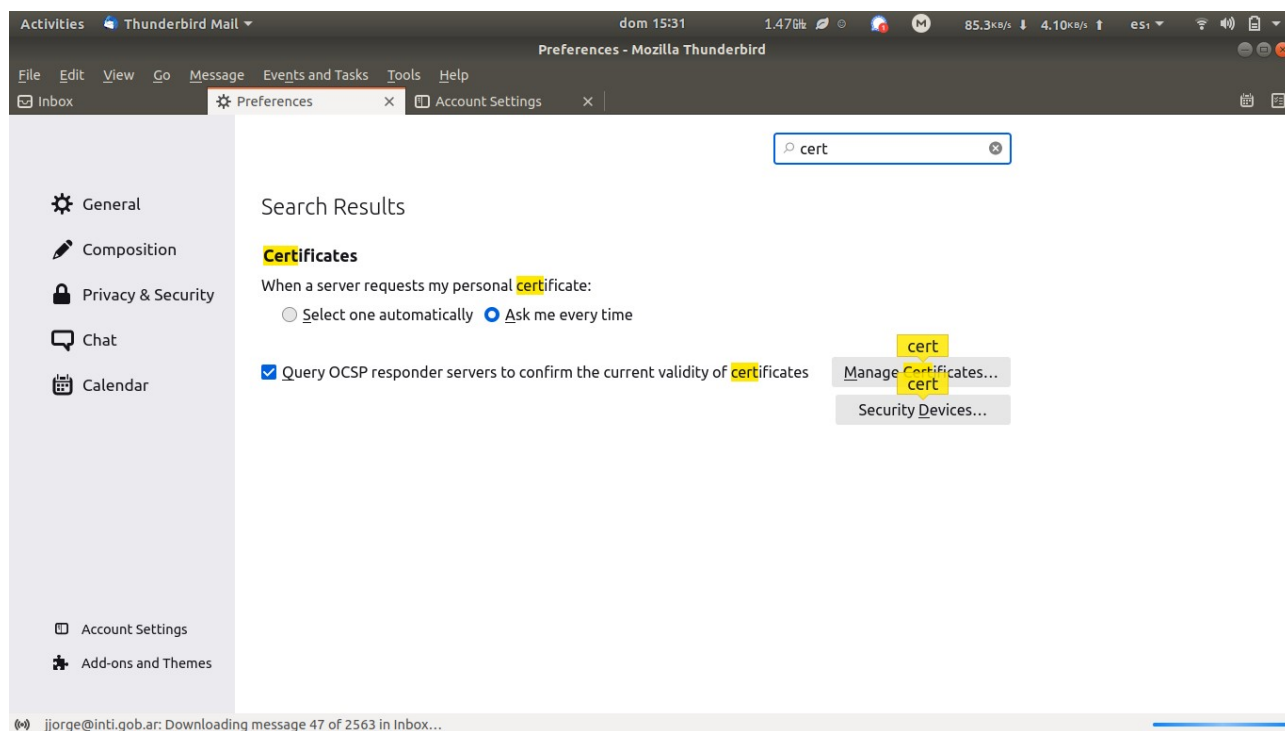
Actalis provee certificados para correo electrónicos gratuitos... pero tienen un problema a ver si lo descubren.

Una vez que validen el correo copien la contraseña que les mostrará el sitio web.



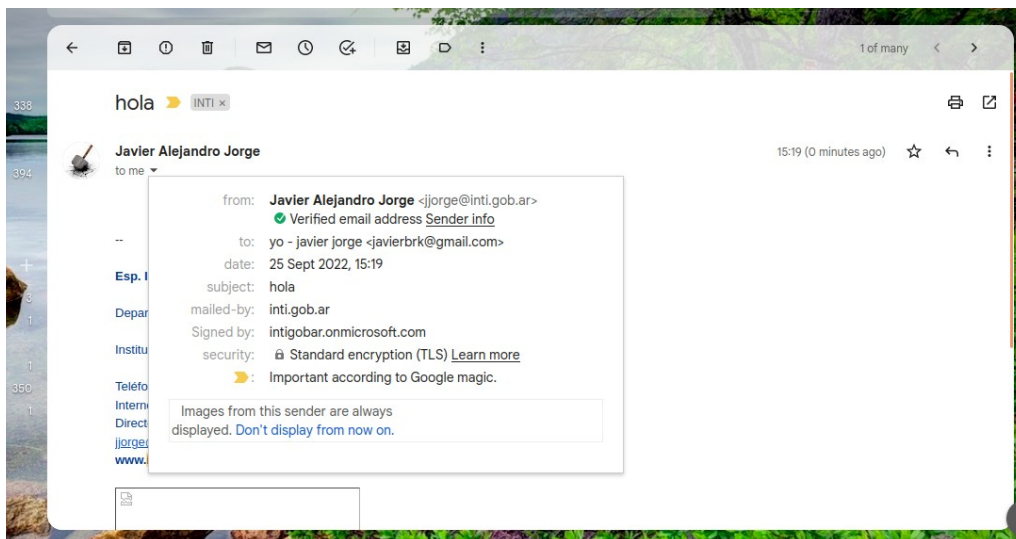
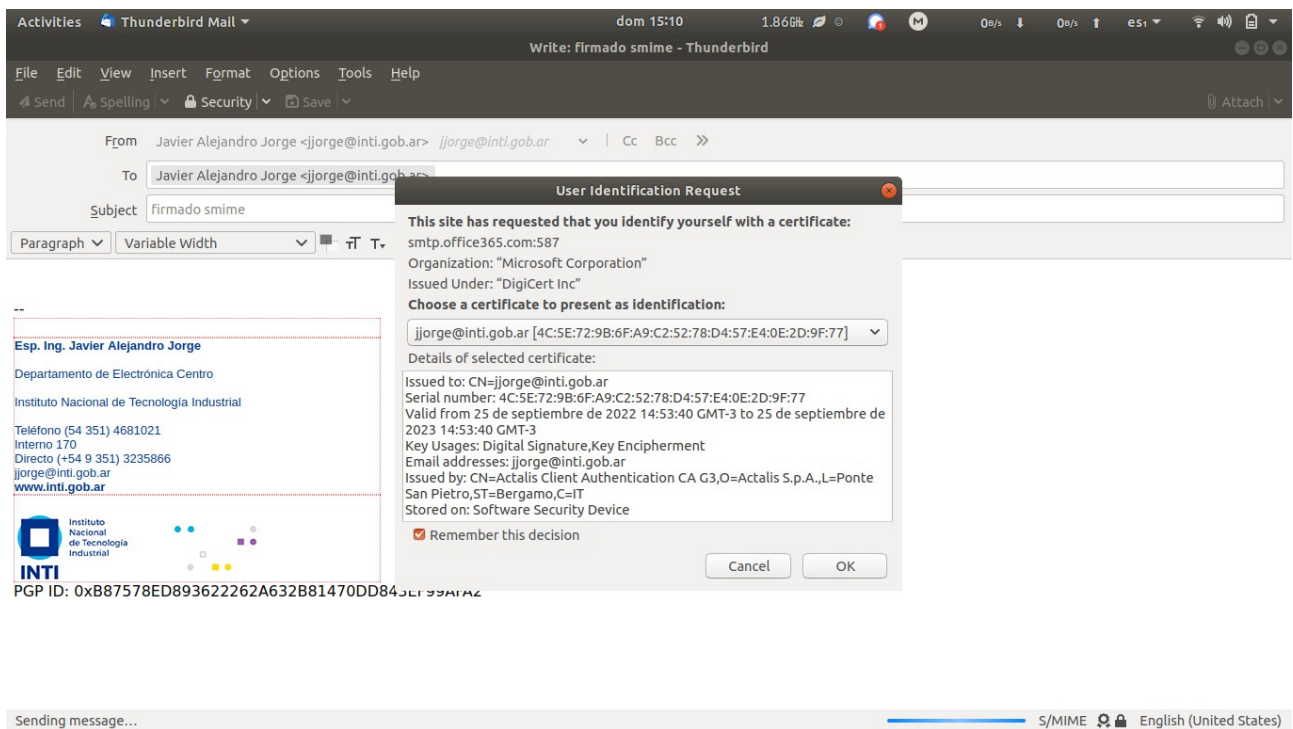
The screenshot shows a web browser window with the URL <https://extrassl.actalis.it/portal/uapub/doSendEmail>. A green notification box at the top states: "We sent you a email, please check your email and enter the code that we sent you in the Verification code field." Below this, the heading "Free Email Certificate" is displayed, followed by a link to "Certificates for S/MIME secure electronic mail". The section "Step 2 - Request Certificate" contains a "Verification code" input field. Below the input field are links for "Free S/MIME Certificates Terms & Conditions", a declaration checkbox "I declare to have read and accept the above terms and conditions, including the applicable certificate policy.", and a link for "Approval of specific clauses related to Free S/MIME Certificates".

Descargar el certificado, descomprimirlo e importarlo desde la opción preferencias, certificados, gestionar certificados.



En la pestaña tus certificados elegir importar.

Luego podrán firmar sus correos



Ref: <https://www.dannyguo.com/blog/how-to-get-a-free-s-mime-certificate/>