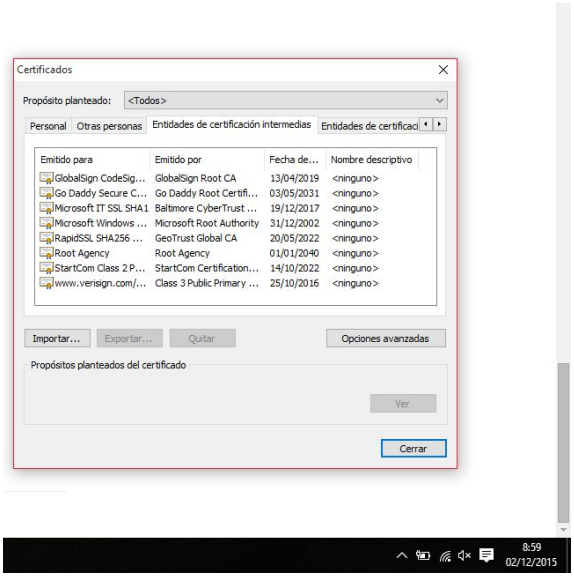
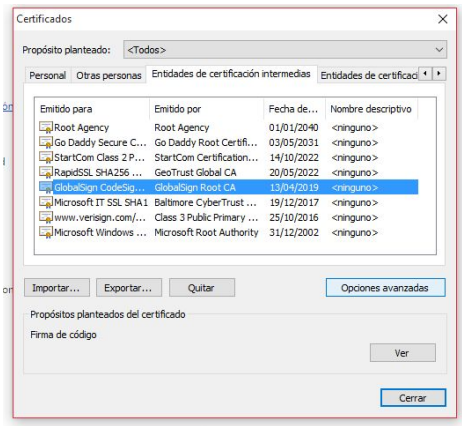
Práctica 7. Certificados Digitales: uso y aplicaciones

1. Acceder a la gestión de certificados de los diferentes navegadores:

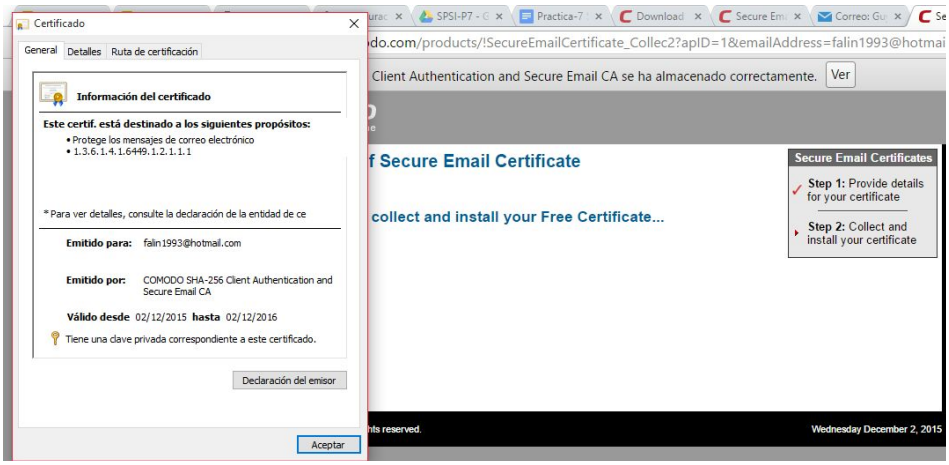


2. Importar con Mozilla una CRL de alguna CA, por ejemplo: http://crl.globalsign.net/Root.crl de GlobalSign

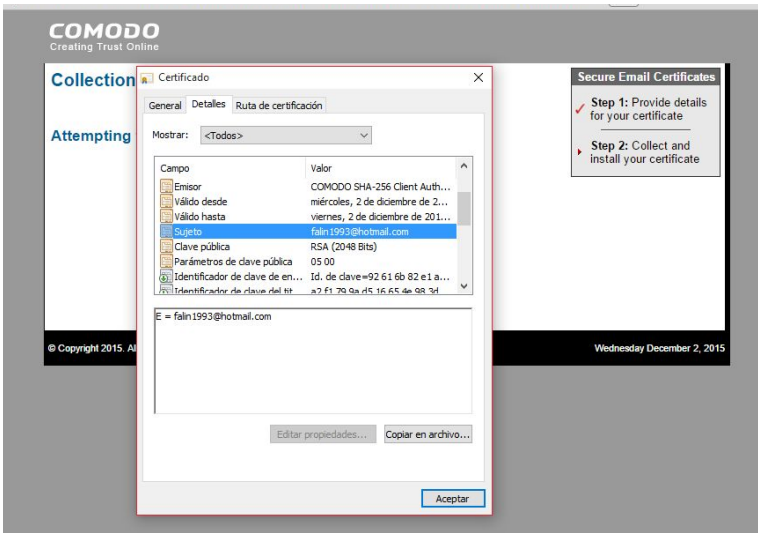


3. Comprobar el aspecto externo de un certificado EV-SSL en: http://www.tbs-certificates.co.uk/comparatif_certificat_serveur_ssl_ev.html.en

4. Obtener un certificado digital clase 1 en modo de prueba de alguna CA (Comodo, GlobalSign, …)

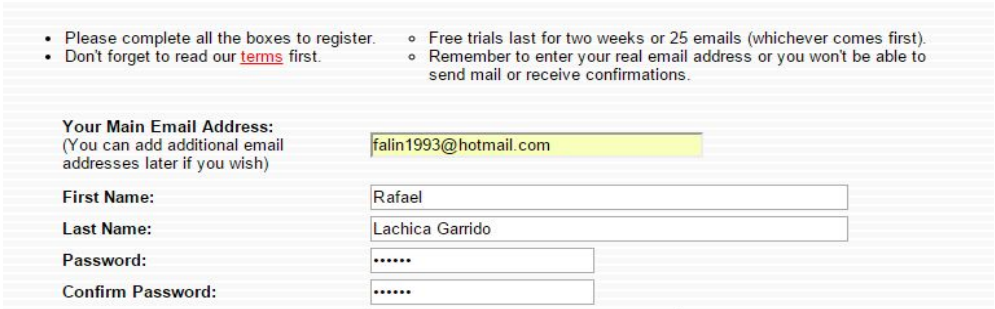


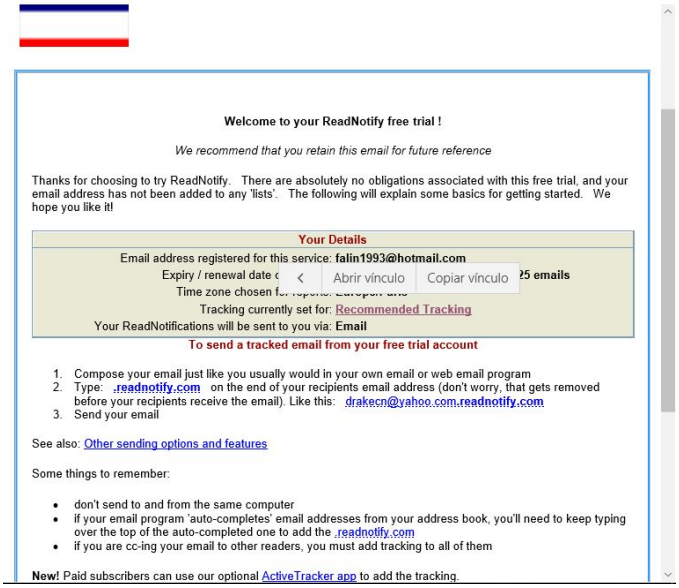
Detalles del certificado:



Emisor: COMODO
Clave pública: RSA(2048 bits)
Sujeto: email

5. Obtener correo con acuse de recibo certificado. Ir para ello a la página de ReadNotify, (http://www.readnotify.com) y registrarse como usuario. Pedir el producto a prueba y comprobarlo en un envió de correo, redirigido a través de su web.





Welcome to your ReadNotify free trial !

We recommend that you retain this email for future reference

Thanks for choosing to try ReadNotify. There are absolutely no obligations associated with this free trial, and your email address has not been added to any 'lists'. The following will explain some basics for getting started. We hope you like it!

Your Details

Email address registered for this service: **falin1993@hotmail.com**
Expiry / renewal date c… **25 emails**
Time zone chosen f…
Tracking currently set for: Recommended Tracking
Your ReadNotifications will be sent to you via: **Email**

Abrir vínculo | Copiar vínculo

To send a tracked email from your free trial account

1. Compose your email just like you usually would in your own email or web email program
2. Type: **.readnotify.com** on the end of your recipients email address (don't worry, that gets removed before your recipients receive the email). Like this: drakecn@yahoo.com.readnotify.com
3. Send your email

See also: Other sending options and features

Some things to remember:

- don't send to and from the same computer
- if your email program 'auto-completes' email addresses from your address book, you'll need to keep typing over the top of the auto-completed one to add the .readnotify.com
- if you are cc-ing your email to other readers, you must add tracking to all of them

New! Paid subscribers can use our optional ActiveTracker app to add the tracking.

Enviamos un correo:

← Responder ≪ Responder a todos → Reenviar Archivar Elim

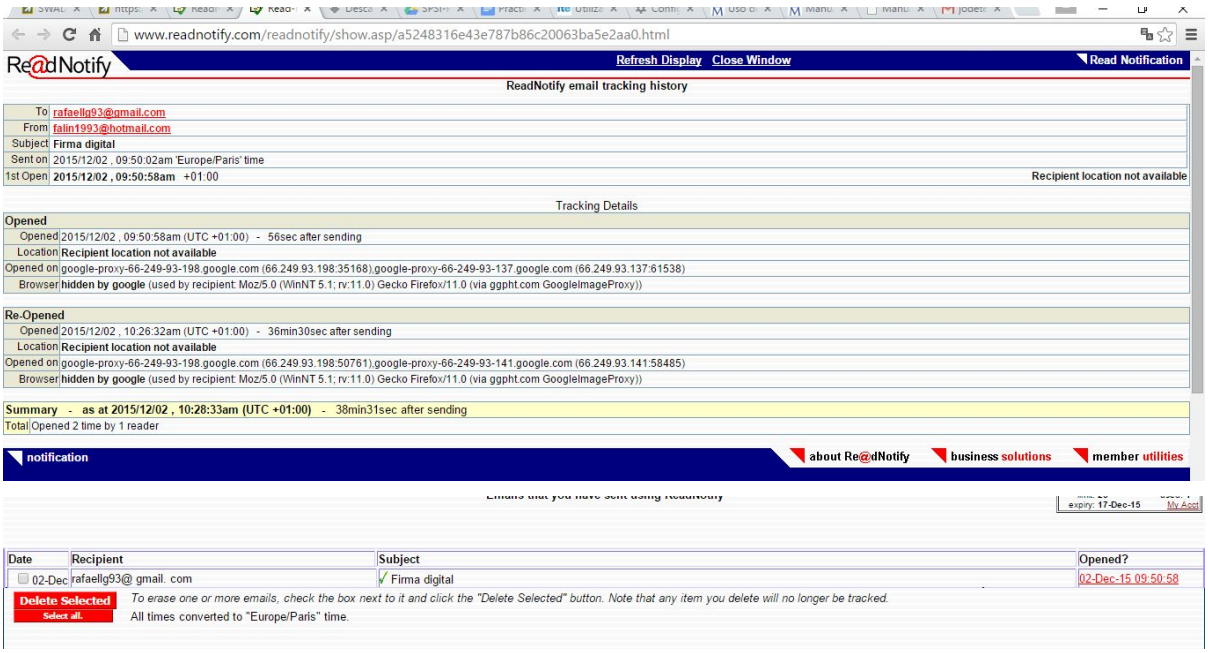
GA Guy Fawkes Anonymous
9:49

Firma digital
Para: rafaellg93@gmail.com.readnotify.com

Firmando un correo

Enviado desde Correo para Windows 10

Añadimos al destinatario el dominio .readnotify



www.readnotify.com/readnotify/show.asp/a5248316e43e787b86c20063ba5e2aa0.html

ReadNotify | Refresh Display | Close Window | Read Notification

ReadNotify email tracking history

To	rafaellg93@gmail.com
From	falin1993@hotmail.com
Subject	Firma digital
Sent on	2015/12/02 , 09:50:02am 'Europe/Paris' time
1st Open	**2015/12/02 , 09:50:58am** +01:00 — **Recipient location not available**

Tracking Details

Opened	
Opened	2015/12/02 , 09:50:58am (UTC +01:00) - 56sec after sending
Location	**Recipient location not available**
Opened on	google-proxy-66-249-93-198.google.com (66.249.93.198:35168),google-proxy-66-249-93-137.google.com (66.249.93.137:61538)
Browser	**hidden by google** (used by recipient: Moz/5.0 (WinNT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggpht.com GoogleImageProxy))

Re-Opened	
Opened	2015/12/02 , 10:26:32am (UTC +01:00) - 36min30sec after sending
Location	**Recipient location not available**
Opened on	google-proxy-66-249-93-198.google.com (66.249.93.198:50761),google-proxy-66-249-93-141.google.com (66.249.93.141:58485)
Browser	**hidden by google** (used by recipient: Moz/5.0 (WinNT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggpht.com GoogleImageProxy))

Summary - **as at 2015/12/02 , 10:28:33am (UTC +01:00)** - 38min31sec after sending
Total: Opened 2 time by 1 reader

notification | about Re@dNotify | business solutions | member utilities

expiry: 17-Dec-15 My Acct

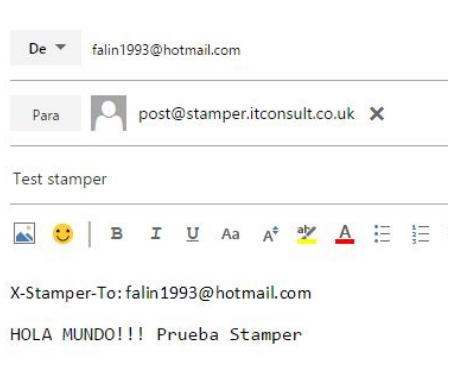
Date	Recipient	Subject	Opened?
02-Dec	rafaellg93@ gmail. com	✓ Firma digital	02-Dec-15 09:50:58

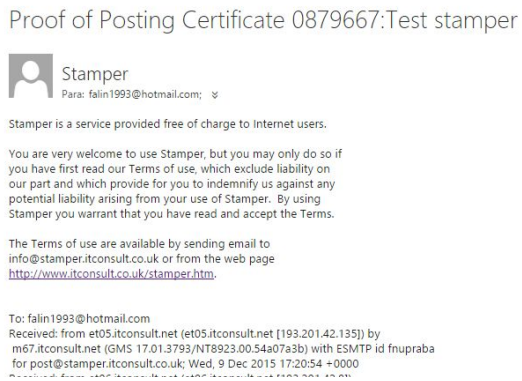
Delete Selected / Select all.

To erase one or more emails, check the box next to it and click the "Delete Selected" button. Note that any item you delete will no longer be tracked.

All times converted to "Europe/Paris" time.

6. Obtener un correo firmado y con sello de tiempo mediante sistema PGP en http://www.itconsult.co.uk/stamper.htm. Para ello remitir el correo a la dirección indicada en la página con X-Stamper-To: destino@correo.dominio. Bajar la Llave Pública del servicio, importarla al anillo de llaves y comprobar que la firma de tiempos es correcta. Probar con las otras opciones del servicio



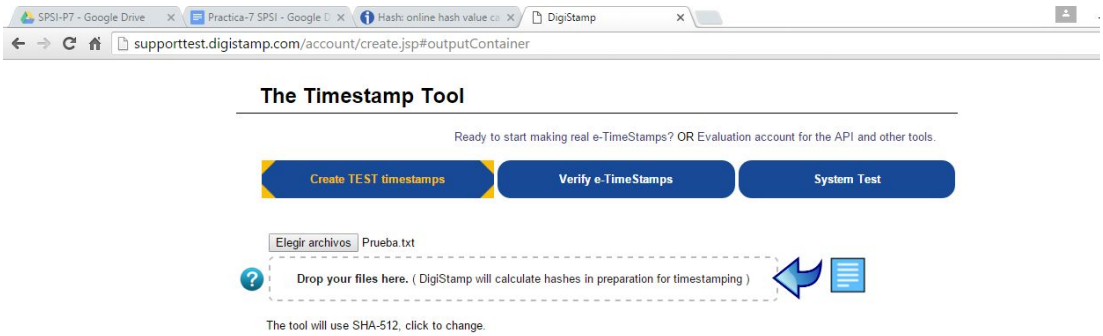


Mandamos el correo a post@stamper.itconsult.co.uk Recibimos el correo con la clave:

-----BEGIN PGP SIGNATURE-----
Version: 2.6.3i
Charset: noconv
Comment: Stamper Reference Id: 0879667

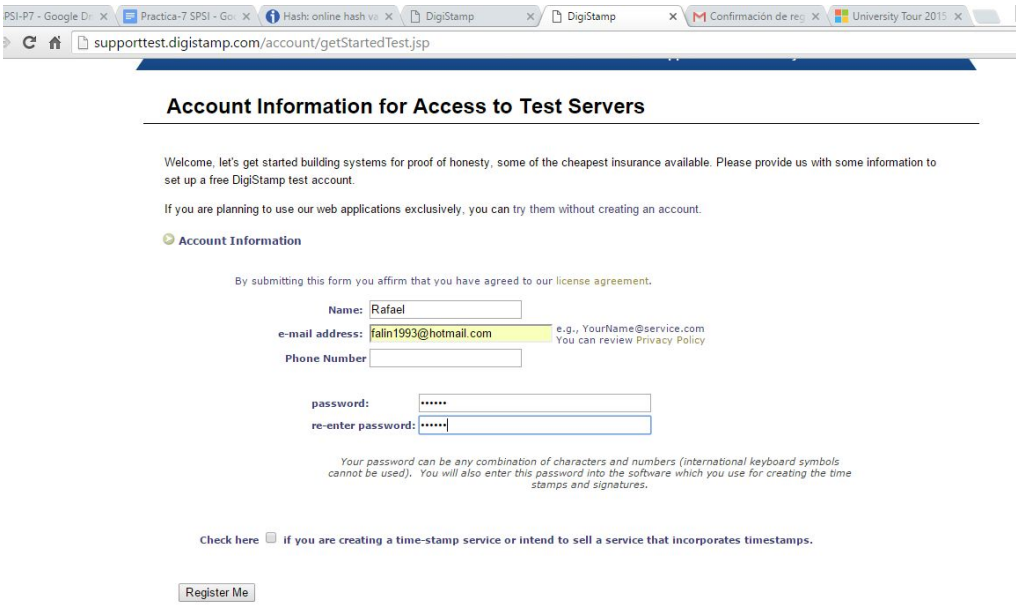
iQEVAgUBVmhj94GVnbVwth+BAQG9mQf+l0cfuaeJfubimCgh0zdG7m09XmAx+4Fl
DwaWzZaTEyxJtRAxTd6nPY180gszc92KZYfO9aQom29s4/F8j/5ukE+AkBk2WoSQ
c0/2KwweyBCjKXyRXMXxuUPaLsAlwij4OELgN6pxzaJE2K87XdfoygtQmZEQalaH
pVwL3swgxmiDxLJdGGcYRaP4jOYeGGYtRdVO4lmMdLVKvMAohXZuqTZP2p3Roqbz
u/7+k4yWPjZlo5ogX4uQdvolKddAK+R+jYxkqJUVCWTbtNLL1s5bGm4NRboHNFp/
X+VlrJ8CHkc1+tfzliby01TTfAeK+x/2a/QgmUbGr8YKXPiYFadCtg==
=aGgs
-----END PGP SIGNATURE-----

7. Utilizar el servicio de sellado de tiempos de e-timestamp https://www.digistamp.com/, probando con cálculo del Hash online, o suministrado por uno mismo mediante las funciones hash provistas en software. Realizar la verificación del sello.



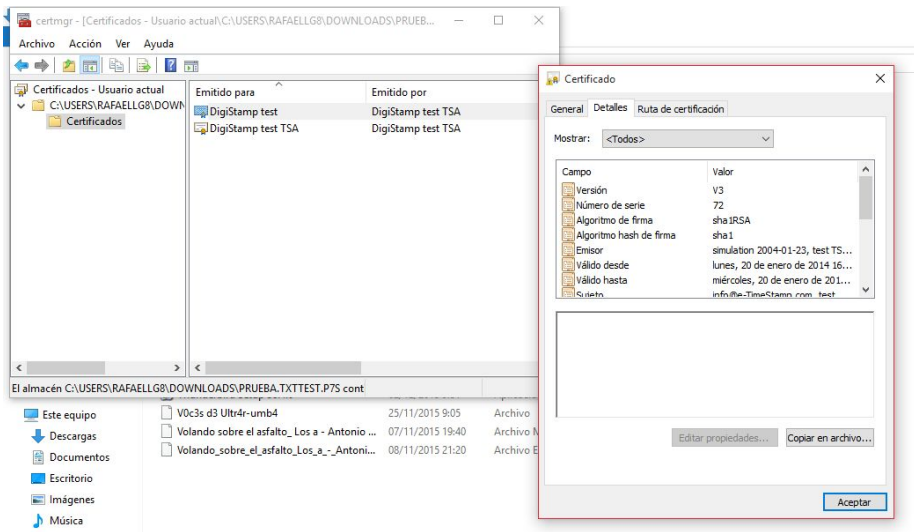
Elegimos el fichero para realizar el sellado con digistamp

Le damos al botón verde de timestamp, y depués nos pedirá que registremos, seleccionamos la opción gratuita:

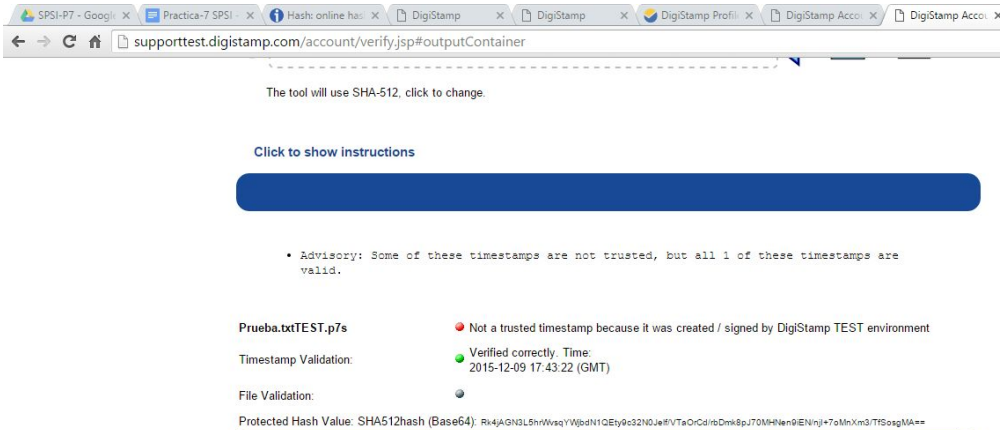


Nos da las claves para realizar las pruebas:

Ahora nos logueamos y creamos nuestro digistamp y obtenemos un archivo "**.p7s**":

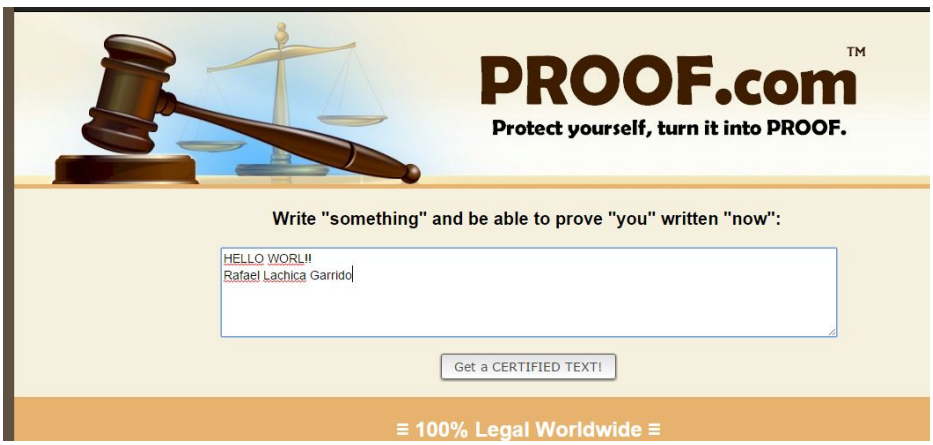


Ahora le damos a verify y seleccionamos el archivo:



Nos da un warning porque dice que el entorno es de tipo TEST gratuita, pero verifica la clave correctamente.

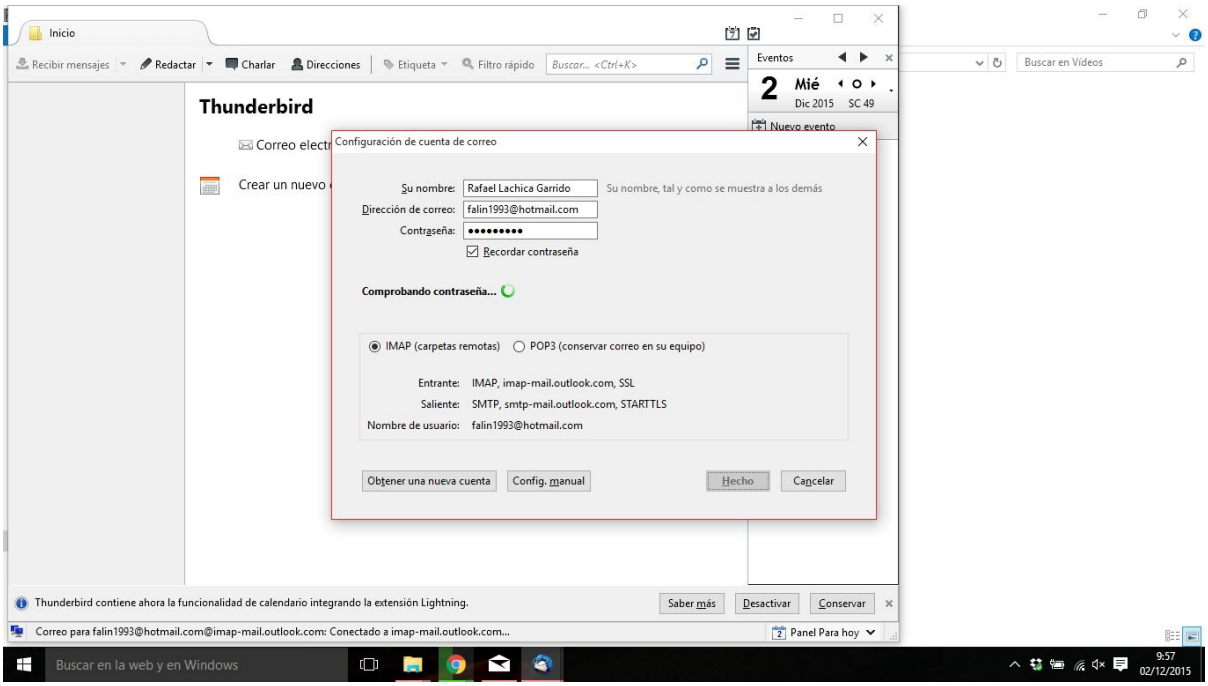
8. El servicio de Proof https://www.proof.com/ provee de certificación y sellado de tiempos instantáneo en la web, con la posibilidad de dejar la certificación a una autoridad descentralizada mediante cadenas de Bitcoins (opción bajo pago).



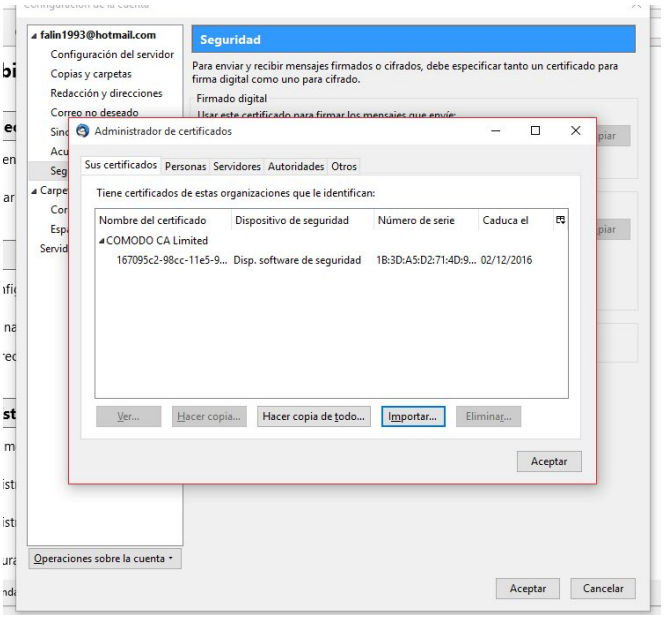
9. El servicio de Registro de la Propiedad Intelectual de http://www.safecreative.com/, Safecreative, ofrece el registro gratuito de hasta 15 obras. Incluye certificados de registro y servicio de sellado de tiempos, aunque algunas de las opciones solo en la modalidad comercial. La página de hashs de sellos de tiempo puede consultarse en http://tsa.safecreative.org/.

10. E-mail seguro. Hacer un ejemplo de cifrado y firmado de correo electrónico con el Certificado Digital de clase 1 obtenido anteriormente en 4. El gestor de correo debe de ser de tipo SMTP/POP3 y admitir S/MIME como protocolo. Por ejemplo Mozilla Thunderbird, Eudora OSE, …

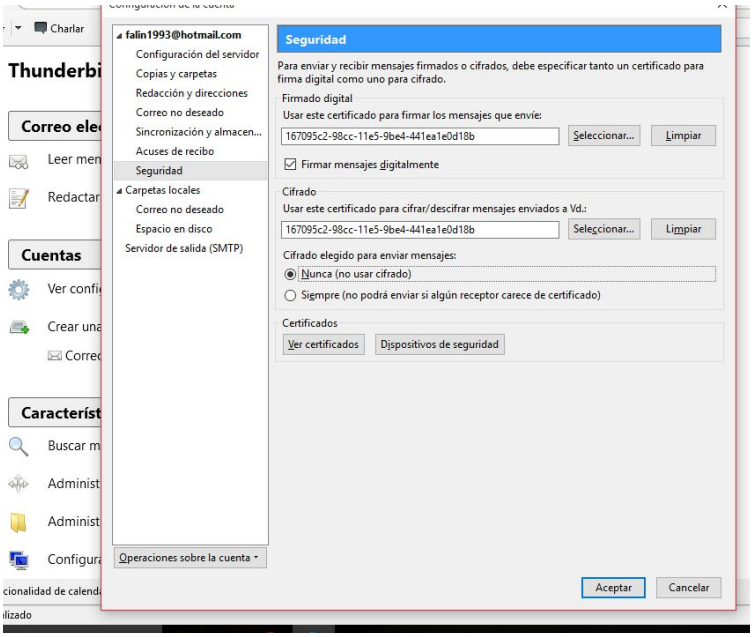
Configuramos Thunderbird



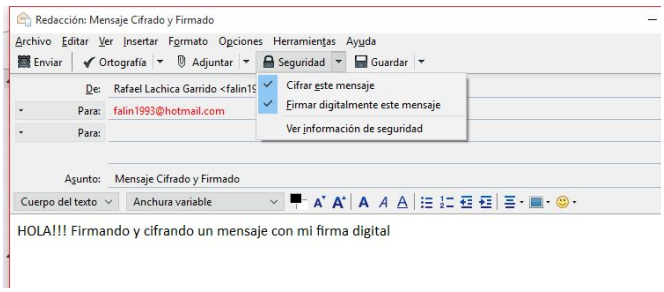
Exportamos la clave privada que instalamos antes y la añadimos a los certificados en Thunderbird:



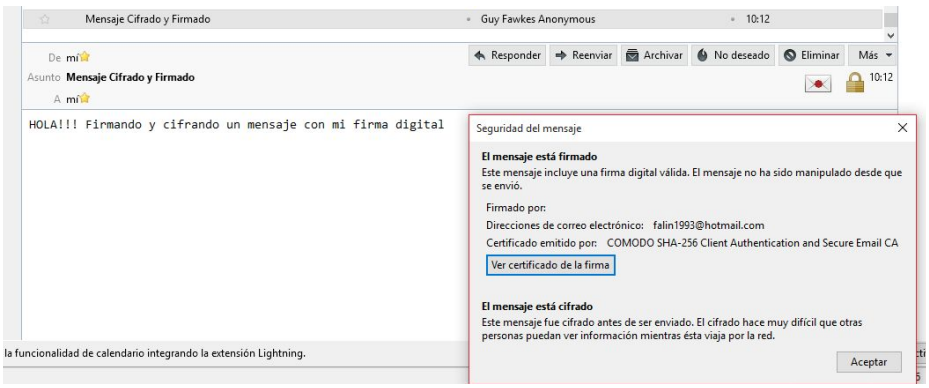
En Seguridad, elegimos nuestro certificado importado:



Creamos el mensaje:



Y ya tenemos nuestro mensaje enviado y recibido firmado digitalmente:

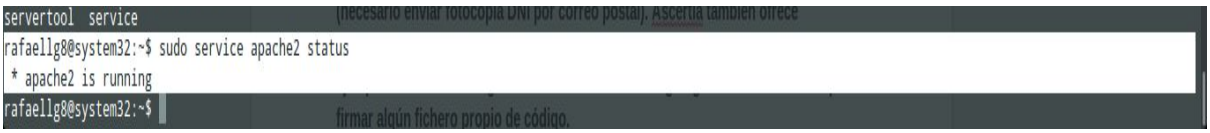


11. Navegación segura mediante certificados SSL.

a. Montar un servidor Apache (puedes hacerlo desde algunos programas que ya lo incluyen como XAMPP, EasyPHP y otros que instalan Apache, PHP y MySQL) .

b. Obtener un CSR (Certificate Signing Request, será la “huella dactilar” de nuestro servidor), lo cual puedes hacer con OpenSSL, por ejemplo, generando primero una pareja de llaves para el servidor, y luego el CSR para las llaves generadas anteriormente.
c. Obtener un certificado SSL en modo de prueba de alguna CA (VeriSign, GlobalSign, Thawte, …). En el proceso deberás de introducir el CSR generado antes. Seguir los pasos indicados.
d. Instalar el certificado SSL obtenido en Apache.
e. Instalar el certificado de la CA que expide nuestro certificado SSL en el navegador para poder enlazar la cadena de confianza y permitir la navegación segura. Este es un certificado de tipo intermedio, especial para la emisión de certificados SSL de prueba, que a su vez se certifica con el Certificado CA Root, o con un certificado Trial Root especial de prueba, que será, eventualmente, también necesario instalar en nuestro navegador si no es distribuido con el mismo.
f. Editar el archivo de configuración de Apache httpd.conf para indicarle los paths a nuestros certificados y llaves y activar ssl si esta no está ya activado.
g. Montar una página web de prueba con dirección localhost (127.0.0.1), y acceder a ella con protocolo SSL mediante el certificado instalado.
h. Instalar un certificado EV-SSL, y realizar la navegación con él.

a) Servidor apache lo tenemos ya instalado en linux:



b) En linux lo creamos a través de los comandos:

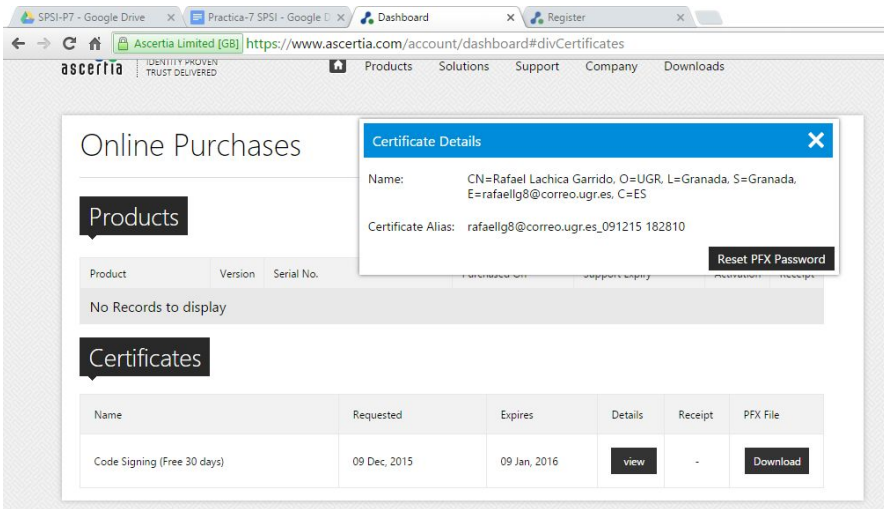
http://www.rackspace.com/knowledge_center/article/generate-a-csr-with-openssl

c)

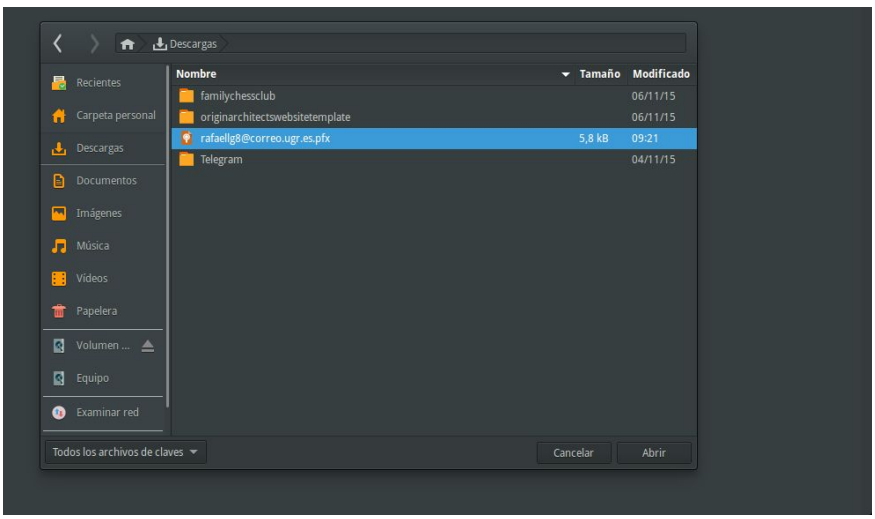
12. Certificados de firma de Código.
Obtener un Certificado Digital de Firma de Código (Code-Signing) Open Source de Certum para publicar código bajo licencia Open Source con periodo de validez 1 año (necesario enviar fotocopia DNI por correo postal). Ascertia también ofrece certificados Code-Signing de prueba por un periodo de validez de 1 mes. Hacer un

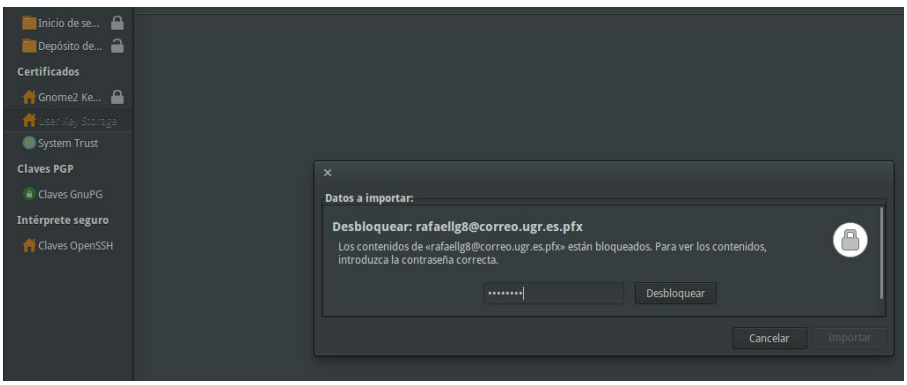
ejemplo de firma de código con el certificado Code-Signing obtenido así. Tomar para firmar algún fichero propio de código.

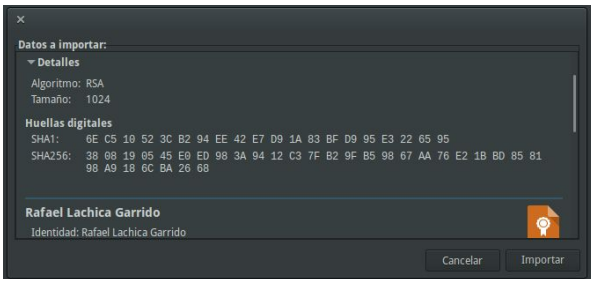
Nos registramos y elegimos un certificado de prueba de 30 días.



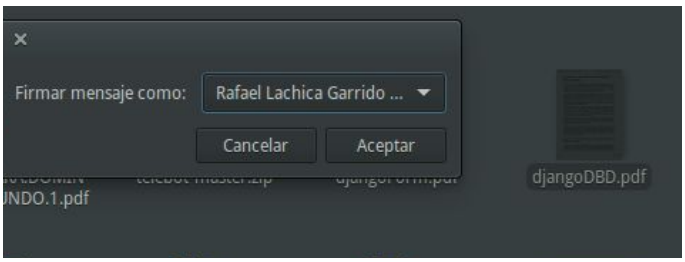
Ahora, a través de las claves de Gnome, por ejemplo, importamos la clave que hemos descargado previamente:







Ahora seleccionamos un fichero, por ejemplo un pdf, (como tenemos instalado seahorse-nautilus), pulsamos botón derecho y ciframos:



Nos crea un archivo .sig, lo abrimos y verificamos la firma: