

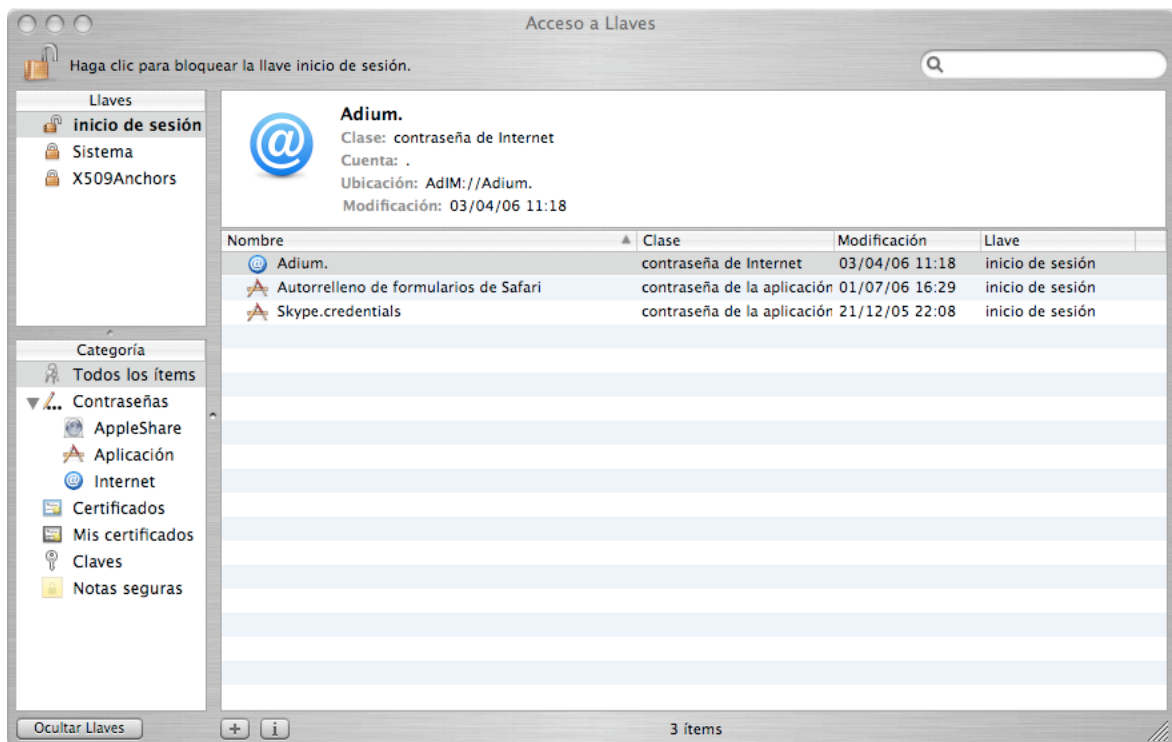


Sección 1 Acceso a llaves



Este es el programa que guarda todas nuestras contraseñas, se encuentra en la sección **utilidades**. Por ejemplo, cuando en el programa Adium o Skype (o tantos otros) usamos nuestra cuenta por primera vez tras introducir la contraseña nos indica si queremos guardarla, si indicamos que si, la contraseña se guarda en el Acceso a llaves, de este modo, cuando usemos de nuevo esa cuenta, el programa leerá la contraseña del acceso a llaves y no nos la pedirá de nuevo.

Si abrimos el programa vemos lo siguiente.



Arriba a la izquierda tenemos las distintas llaves que existen:

- La llave de inicio de sesión se encuentra abierta por defecto, para que los programas puedan añadir información a ella cuando le damos a “guardar contraseña”. Es propia de cada usuario y es la llave que se usa por defecto y la más importante.
- La llave de sistema guarda claves asociadas a distintos usuarios, como por ejemplo la contraseña de airport de distintas redes.

- La llave X509Anchors guarda los certificados digitales que van preinstalados en el sistema. Mas tarde explicaré que son los certificados.

En la sección categoría podemos filtrar los items que tenemos a la derecha, por contraseñas de internet, de aplicación, certificados, claves, etc..

Por cada contraseña que guardamos se crea un item a la derecha, en mi captura se puede ver un item de Adium, y otro de Skype. Los items de aplicación tienen un símbolo distinto a los items de web.

Finalmente también podemos filtrar los items por nombre arriba a la derecha, como de costumbre en las aplicaciones Mac.

Los items de contraseña se pueden editar dando doble clic, y también borrar. Si borramos un item, la aplicación que lo usa no podrá leerlo y volverá a pedirnos contraseña como la primera vez que la usamos. En ese caso, de nuevo, podremos indicarle si queremos que ésta se guarde en el acceso a llaves.

Si nunca has tenido problemas ni curiosidad por saber como funciona más en detalle esta aplicación, puedes seguir viviendo sin conocerla más, y, además puedes firmar tus emails sin saber mucho más, de modo que pasaré al siguiente apartado, para, más tarde, volver a esta aplicación para que las personas que tengan curiosidad puedan aprender un poco más.



Sección 2 Conceptos de seguridad

Aquí explicaré algunos conceptos de seguridad informática.

Certificado o entidad digital es una manera de identificar a alguien en forma electrónica. Consta de un código secreto (tu "clave privada") y otra clave la cual uno publica libremente (tu "clave pública"). Tu clave privada te permite firmar documentos electrónicos, y todas las personas que lo lean podrán verificar tu firma usando tu clave pública. Del mismo modo, con tu clave privada puedes mostrar ("desencriptar") documentos que otros usuarios ocultaron ("encriptaron") usando tu clave pública.

De este modo uno puede publicar su clave publica en un servidor de claves, o bien colocarla en su web, de este modo todas las personas que dispongan de ella podrán: confirmar que somos nosotros quienes le escribimos, osea comprobar nuestra firma electrónica en un email, y también enviarnos información que solo podremos leer nosotros (información encriptada con nuestra clave publica que solo puede ser desencriptada con nuestra clave privada).

Para asegurar la autenticidad de una identidad digital, las autoridades certificadoras suministran identidades digitales a individuos, cuyas identidades pudieron ser verificadas.

Una autoridad certificadora (CA): es una identidad digital que firma certificados (como Verisign). Emiten certificados de diferentes niveles, formando lo que se conoce como "cadena de certificación". Para que un certificado sea válido, la CA que lo firmó debe ser válida, y lo mismo se aplica a toda la cadena. La validez de los certificados de una cadena es determinada en forma automática por el Mac OS X, al evaluar un certificado.

Esto quiere a decir a nivel práctico que si Verisign certifica a la entidad keroCA y keroCA hace un certificado a jack kerouack, el certificado de jack será fiable para nosotros ya que ha sido certificado por una entidad fiable (keroCA) y, a su vez, keroCA es fiable porque ha sido certificada por Verisign, que es raíz y fiable. Las CAs raíz son las mas importantes, se confía en ellas y crean su propio certificado fiable. En el acceso a llaves, llave X509Anchors, ya se encuentran multitud de certificados aceptados de entidades certificadoras importantes, como Verisign, esto provoca que todo lo certificado por Verisign, o por otra entidad que fuera certificada por Verisign, es fiable para nosotros. Podemos conseguir mas certificados de entidades fiables y añadirlos.

Para firmar un email: Necesito un certificado, con su clave publica y su clave privada. Conceptualmente existen dos formas de asegurar la fiabilidad de la firma:

- Dar la clave pública de forma segura a nuestros “amigos” (desde un servidor, o nuestra web, en persona o email). Cuando reciban un email firmado con nuestra clave privada, comprobarán la firma con nuestra clave pública. De este modo no hace falta que el certificado lo haya creado una CA certificada, podemos generarlo nosotros mismos.

- Obtener el certificado de una CA certificada, de este modo no hace falta que demos la clave pública a nuestros amigos. Como ya dije, si Verisign certifica a Thawte (otra CA) y Thawte nos certifica a nosotros, cualquier persona que confíe en Verisign (osea todo el mundo), confiará en nuestro certificado.

Por otro lado existen dos niveles de certificación, en el primero se asegura que escribe el email la persona dueña de la cuenta de email, en la segunda modalidad, además de lo primero se conoce quien es exactamente la persona dueña del email con nombre y apellidos.

¿Pero realmente sirve de algo la primera opción?

Aunque en la primera opción no tengamos certeza a nivel de seguridad informática de quien es quien nos escribe el email, puede que ya dispongamos de esta información. Por ejemplo, yo uso una determinada dirección de correo, mis amigos conocen mi dirección y también me conocen a mi y saben quien soy. Sin embargo cualquier persona puede enviarles un email en el que figure mi dirección en el apartado de remitente. sin embargo, si yo les aviso de que a partir de ahora firmaré mis emails, ellos tendrán la seguridad de que si mi email está firmado, es seguro que lo estoy enviando realmente yo.

Otro ejemplo, si recibimos un email firmado desde una dirección de una gran empresa, puede que no sepamos con nombre y apellidos quien exactamente nos escribe , pero sabremos que es realmente el dueño del email, y, por tanto, se nos escribe desde esa empresa realmente y no es una broma de un amigo, envío de virus o propaganda.

Para encriptar un email : Necesitamos tener nuestro certificado y, además, tener el certificado de la persona a quien le enviamos el email. Explicación técnica: Necesitamos la clave pública de la persona que será la única que pueda leerlo. De este modo lo ocultaremos con su clave pública, y como esta persona es la única que tiene su clave privada, será la única que pueda leerlo.



Firma digital en MAIL paso a paso



Voy a explicar paso a paso el proceso de solicitar un certificado digital para nuestro email a una entidad certificadora. Este certificado autentificará que la persona que escribe el email es la dueña de la cuenta. Para, además, certificar quien es la persona dueña de la cuenta se deben seguir otros pasos, e ir a determinadas oficinas con nuestro DNI para que lo comprueben.

He elegido la autoridad de certificación THAWTE (<http://www.thawte.com>) ya que indagando por internet he sabido que hacen certificados a emails de forma gratuita, es posible que existan muchas otras autoridades que podamos usar.

El proceso de realizar la petición no es corto, pero tampoco especialmente difícil, se trata de leer las indicaciones e ir haciendo lo que corresponda.

En primer lugar entramos en la pagina web y elegimos el idioma español, aunque no toda la información de la página se nos vaya a traducir.



Pulsamos el enlace “Protección de su email” en el apartado “Qué necesita”.

Join

Login

Retrieve lost thawte ID or password

Pulsamos Join.

Nos aparece una ventana nueva con los términos del contrato, los aceptamos pulsando next.

Damos nuestros datos básicos.

Indicamos la cuenta de correo a certificar, y algunos datos más, como el típico apartado de preguntas sencillas, que debemos rellenar para utilizar en caso de que olvidemos nuestro password.

my account

history

ID info

preferences

change password

edit ID info

change thawte ID

▶ X.509 Format Certificates

request

De este modo llegaremos a la página en la cual manejaremos nuestras peticiones de certificados.

Para solicitar un certificado pulsamos en Certificates y luego en Request my certificate.

certificates

Pulsamos en el Request asociado a los certificados X.509. Inicialmente nuestro certificado estará pending, cuando sea creado pasará a estar issued.

my emails

Seguimos los pasos y recibiremos un email con dos claves, tras esto colocamos las dos claves en la página web y se nos indicará una web para descargar el certificado. Pinchamos en el enlace (Fetch) y el certificado se nos añadirá automáticamente a nuestro acceso a llaves, sección “mis certificados”.

wot console



Thawte Personal Freemail Issuing CA

Entidad de certificación intermedia

Caduca: miércoles 17 de julio de 2013 01H59'59" Europe/Madrid

✓ Este certificado es válido



@gmail.com



Thawte Personal Freemail Issuing CA

En este momento abrimos la aplicación Mail y veremos que al escribir un nuevo mensaje disponemos de dos nuevos botones a la derecha de la firma. El candado sirve para encriptar el email, y no podemos usarlo ahora mismo ya que no disponemos del certificado (clave publica) de nadie. La “V” si podemos usarla ya que ya tenemos nuestro certificado, sirve para firmar nuestro email. Si vemos la “V” el email se firmará, si vemos la “X” no se firmará. Pulsamos el botón para cambiar su estado.



Cuando recibamos un email firmado por alguien, el certificado (clave pública) del emisor se añade a nuestro acceso a llaves (podremos verlo en la sección certificados). De este modo cuando le enviemos un email a esta persona, podremos usar el botón del candado para encriptar el email. Candado cerrado indicará encriptado y candado abierto no encriptado.

Cada aplicación tiene una forma de indicarnos que un email está firmado o encriptado, Mail nos lo indica de estos modos:

Seguridad: Firmado

Seguridad: Encriptado

Seguridad: Encriptado, Firmado

Ya podemos asegurarnos de que quien recibe un email, está seguro de que somos nosotros, y, además, enviarle información que sólo él podrá leer (siempre que él también use certificados).

 **smime.p7m**
168K [Descarga](#)

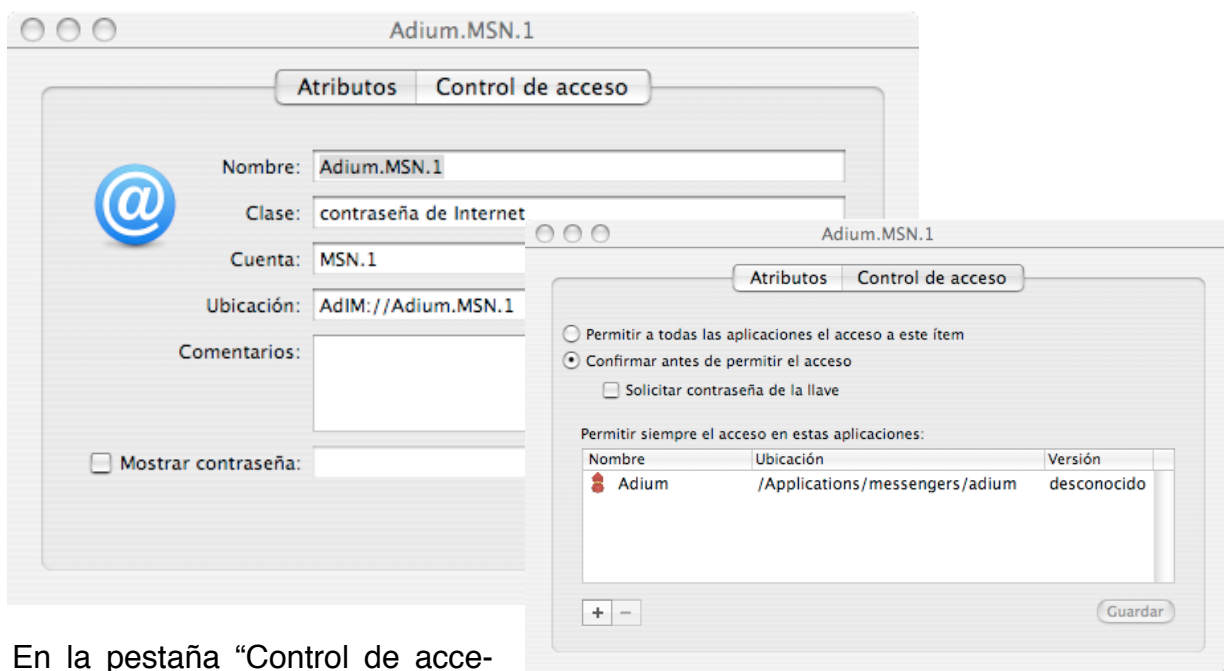
Si recibimos un email firmado en un lector de correo que no reconoce las firmas, como gmail por web, veremos este archivo como adjunto.



Acceso a llaves II, la venganza.

Ya puedes firmar y encriptar emails, además tienes una idea de la aplicación acceso a llaves, de modo que si no te apetece seguir leyendo, tu mismo, yo probablemente no seguiría y me pondría a escuchar un buen disco. Para los demás...

Si pulsamos doble clic sobre un elemento de seguridad del acceso a llaves veremos la siguiente información. Por defecto no se muestra la contraseña asociada a este momento, pero podemos aquí visualizarla.



En la pestaña “Control de acceso” podemos ver que aplicación puede leer este elemento/contraseña, y cambiar algunos de sus atributos, así como añadir aplicaciones que puedan leer este elemento.

El típico mensaje cuando instalamos una nueva versión del mismo programa de “Esta aplicación solicita permiso para leer del acceso a llaves”, quiere decir que se nos pide permiso para añadir la nueva versión del programa aquí, o bien que va a crear un nuevo elemento de llaves con esa información.



Notas seguras

También podemos crear notas con contraseñas de lo que queramos y se guardaran de forma segura