Manual de Instalación
Certificado Digital Izenpe

GNU/Linux
Ubuntu 10.04 – Lucid Lynx

Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490

Indice de contenido

Introducción

Izenpe, en un esfuerzo por apoyar y facilitar el uso de sus certificados a los usuarios de software libre y open source en la Comunidad Autónoma Vasca ha desarrollado diversas guías con el objetivo de detallar los pasos necesarios para instalar y configurar los certificados digitales de Izenpe sobre el sistema operativo GNU/Linux.

En este caso se describirá el proceso a seguir en la distribución Ubuntu 10.04 para lograr utilizar los certificados digitales de Izenpe con las aplicaciones más importantes que dan acceso a los servicios ofrecidos por la administración pública vasca.

Estructura del documento

El documento se estructura en 5 secciones secuenciales que detallan minuciosamente el proceso completo de instalación, configuración y uso de los certificados digitales de Izenpe en GNU/Linux:

- Instalación de drivers para la tarjeta criptográfica de Izenpe
- Configuración de los distintos lectores soportados
- Configuración de las distintas aplicaciones soportadas
- Instalación de los certificados de las autoridades certificadoras en las aplicaciones
- Ejemplo de uso de las aplicaciones

Cada una de estas secciones explica las tareas necesarias para llevar a cabo el proceso completo.

Alcance del documento

Este documento pretende servir de manual de instalación para todas aquellas distribuciones tipo Debian, caracterizadas por disponer de paquetes .deb y la herramienta de gestión de paquetes apt-get y/o aptitude.

El proceso que se ha documentado es específico para Ubuntu 10.04 pero el resto de distribuciones similares, como Debian GNU/Linux, Knoppix, Linux Mint, DreamLinux, Morphix... tendrán un proceso de configuración muy semejante al indicado.

Hardware y aplicaciones oficialmente soportadas:

En este documento no es posible dar cabida a todos los dispositivos hardware existentes en el mercado. Por ello desde Izenpe se ha decido dar soporte de manera oficial a los siguientes lectores USB de tarjetas criptográficas:

- Cherry RS 6600 USB (firmware: 1.06)
- Gemplus GemPC Twin (firmware: 1.0)
- BIT4ID ACR38 (firmware: 1.0)
- C3PO LTC31 (firmware: 0.36)

Todos ellos pueden ser adquiridos o a través de la tienda web de Izenpe (http://www.izenpedenda.com/) o en cualquier otro proveedor autorizado. Además otros lectores podrán funcionar siempre según la disponibilidad de drivers.

Para acceder a los servicios ofrecidos por Izenpe es necesario disponer de herramientas y aplicaciones que hagan uso de los certificados de Izenpe. Las aplicaciones más comunes que hacen uso de estos certificados se han agrupado en tres categorías y se ha intentado documentar el proceso de instalación y configuración de las mismas con los certificados de Izenpe.

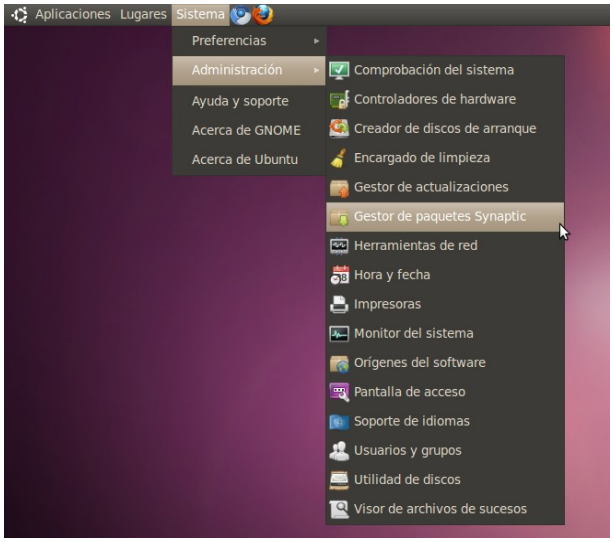
Las aplicaciones que se explicarán en este documento son:

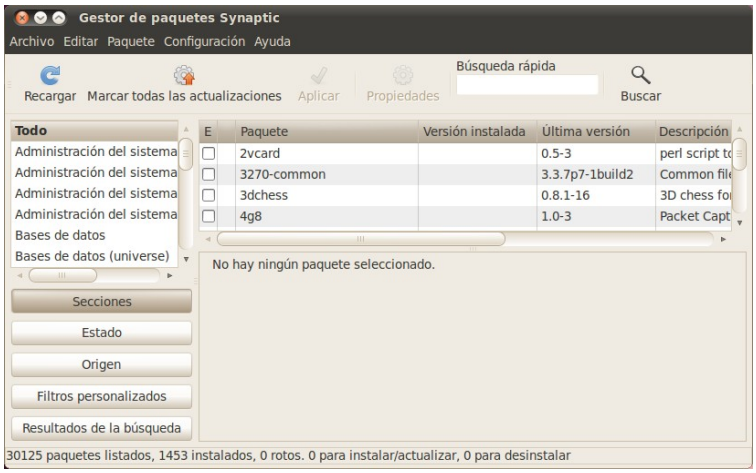
- Navegadores Web
  - Firefox 3.6
  - Opera 10.10
  - Google Chrome / Chromium 5
- Clientes de correo:
  - Thunderbird 3
  - Evolution 2.28
  - Kmail 1.13
- Herramientas Ofimáticas
  - OpenOffice.org 3.2

Observaciones

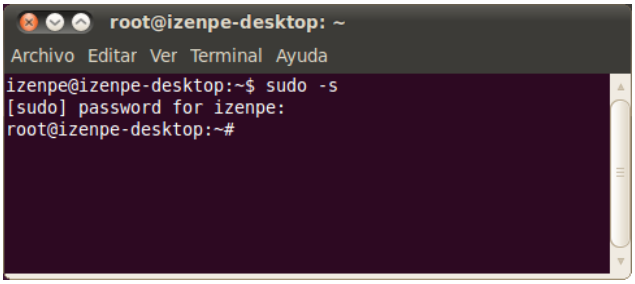
A lo largo del documento será necesario, en algunos casos, la instalación de un determinado software o librerías para poder utilizar los dispositivos hardware. Para dicho proceso se detallarán dos aproximaciones para llevar a cabo las tareas, de las cuales el usuario podrá escoger cual sigue:

- Modo gráfico: a través del entorno gráfico. La instalación gráfica se realizará mediante el software Synaptic





- Modo consola: a través de la línea de comandos. La instalación a través de línea de comandos se realizará mediante el *Terminal*. Algunas acciones que realizaremos requerirán disponer de privilegios de superusuario o "root", por lo que en adelante todas las acciones que así lo requieran se indicarán con una almohadilla (#).

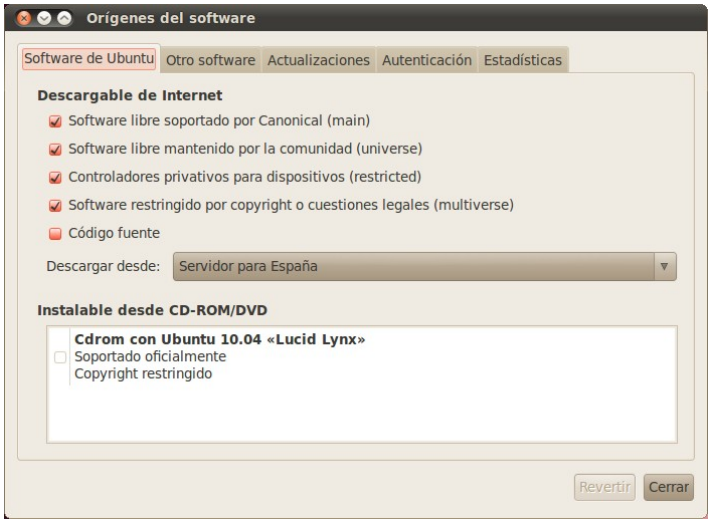


Otras notas

Si bien es cierto que hay pasos que se podrían agrupar en uno solo, el documento trata de explicar paso por paso las distintas acciones a realizar con la finalidad de proporcionar una mayor comprensión en la arquitectura de los certificados digitales y en el proceso de instalación y configuración sobre GNU/Linux.

Para la instalación de los certificados digitales es necesario que el ordenador disponga de acceso a Internet.

Además es necesario comprobar que el sistema tiene acceso a los siguientes repositorios *Universe* de Ubuntu (vienen configurados por defecto) y que podemos comprobarlo en la aplicación Synaptic, Configuración → *Repositorios:*



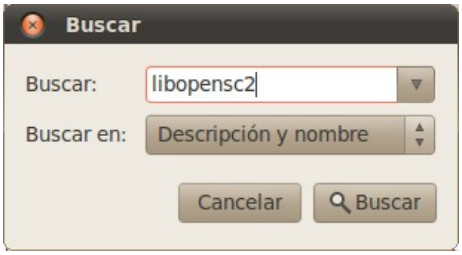
Instalación de los drivers para la tarjeta criptográfica de IZENPE

Los certificados de usuario final emitidos por Izenpe están alojados en una tarjeta criptográfica. Las librerías necesarias para que el sistema GNU/Linux interactúe con los datos alojados en las tarjetas es necesario instalar las librerías *opensc*.

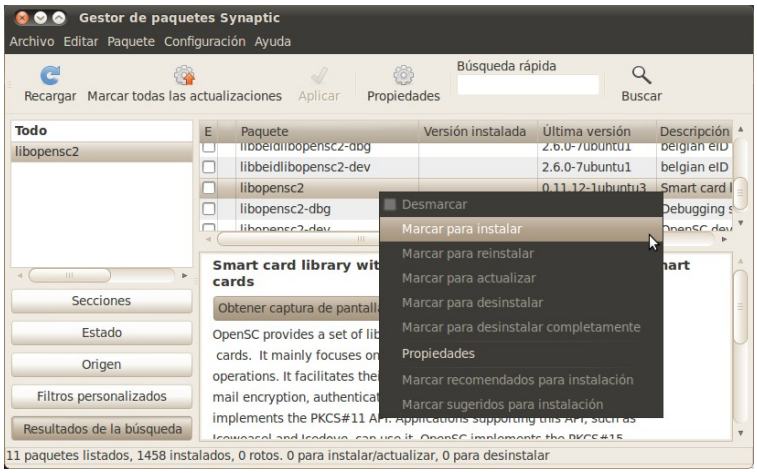
Instalación a través del entorno gráfico

Procedemos a la instalación a través de la herramienta de gestión de paquetes *Synaptic*.

Buscamos el paquete mediante el botón *Buscar* de *Synaptic*:



Indicamos la librería que queremos instalar `libopensc2` y pulsamos sobre *Buscar.* A continuación seleccionamos el paquete y *Marcar para instalar*:



Una vez marcado el paquete para instalar aplicamos los cambios y esperamos a que el proceso se complete.

Instalación a través de la línea de comandos

Abrimos una terminal de línea de comandos y en modo superusuario ejecutamos el siguiente comando:

```
# apt-get install libopensc2
```

Configuración de los lectores

Configuración general

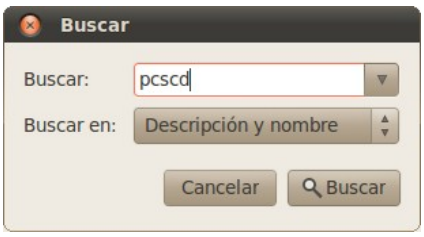
Para que las aplicaciones accedan a los certificados ubicados en las tarjetas los lectores necesitan un software middleware que se encargue de gestionar las transacciones de comunicaciones y datos. Este middleware en GNU/Linux es gestionado a través de un servicio que se encarga de cargar/descargar dinámicamente los drivers de los lectores y gestionar las conexiones a los mismos.

A continuación instalaremos el "demonio" *PC/SC*

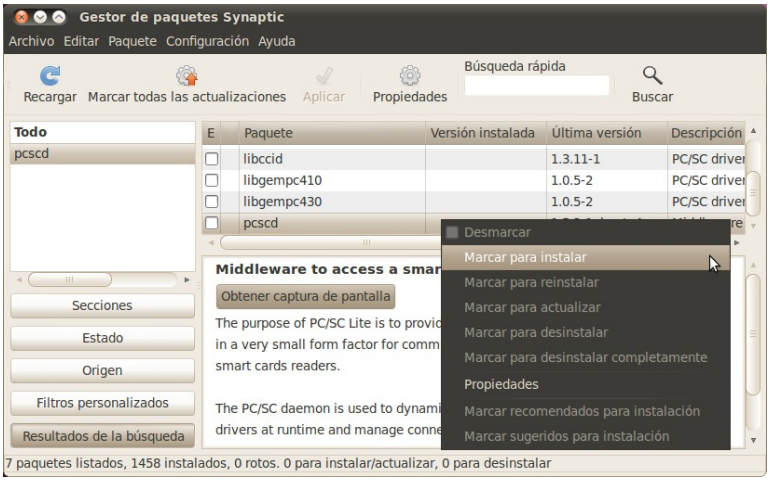
Instalación a través del entorno gráfico

Procedemos a la instalación a través de la herramienta de gestión de paquetes *Synaptic*

Buscamos el paquete mediante el botón *Buscar* de *Synaptic (es necesario maximizar la ventana para poder ver el botón)*:



Indicamos la librería que queremos instalar *pcscd* y pulsamos sobre *Buscar.* A continuación seleccionamos el paquete y *Marcar para instalar*:



Una vez marcado el paquete para instalar aplicamos los cambios y esperamos a que el proceso se complete.

Instalación a través de la línea de comandos

Abrimos una terminal de línea de comandos y en modo superusuario ejecutamos el siguiente comando:

```
# apt-get install pcscd
```

Lectores Cherry RS 6600 USB, GemPlus GemPC Twin, C3PO LTC31 y otros

La librería *ccid*, que implementa el protocolo CCID (Chip Card Inteface Device), intenta dar soporte a la mayor parte de los lectores USB del mercado.

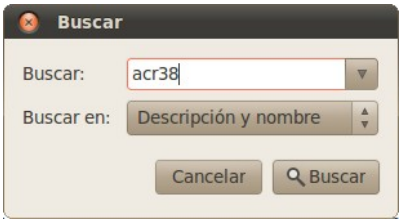
Al instalar *pcscd* nos instalará *libccid* por dependencia, así que no será necesario instalarlo.

Lector BIT4ID ACR38

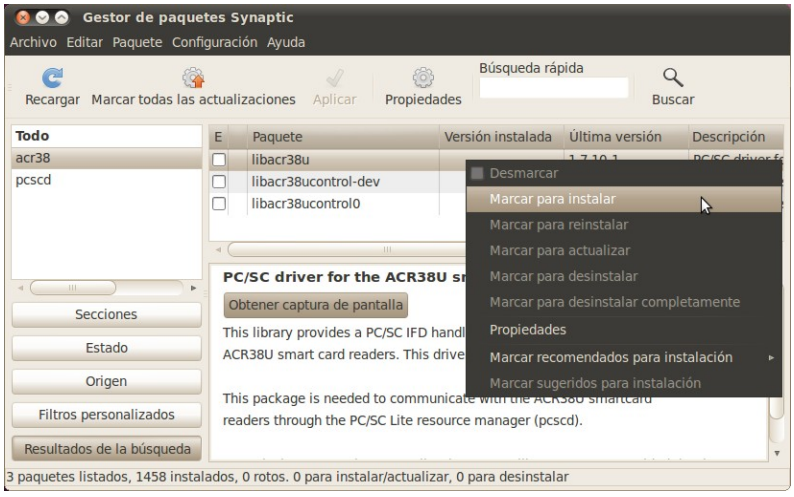
Instalación a través del entorno gráfico

Procedemos a la instalación a través de la herramienta de gestión de paquetes *Synaptic.*

Buscamos el paquete mediante el botón *Buscar* de *Synaptic*:



Indicamos la librería que queremos instalar `libacr38u` y pulsamos sobre *Buscar.* A continuación seleccionamos el paquete y *Marcar para instalar:*



Una vez marcado el paquete para instalar aplicamos los cambios y esperamos a que el proceso se complete.

Instalación a través de la línea de comandos

Abrimos una terminal de línea de comandos y en modo superusuario ejecutamos el siguiente comando:

```
# apt-get install libacr38u
```

Configuración de las aplicaciones

Lamentablemente el sistema operativo GNU/Linux no tiene implementado, a nivel de sistema operativo, una arquitectura centralizada para la gestión de certificados digitales. A día de hoy la implementación más avanzada es la de la suite Mozilla, mediante módulos *PKCS#11* y muchas otras aplicaciones hacen uso de ella, como veremos más adelante.

Navegadores web

Firefox

Firefox es el navegador por excelencia en GNU/Linux.

Instalación de módulo para certificados

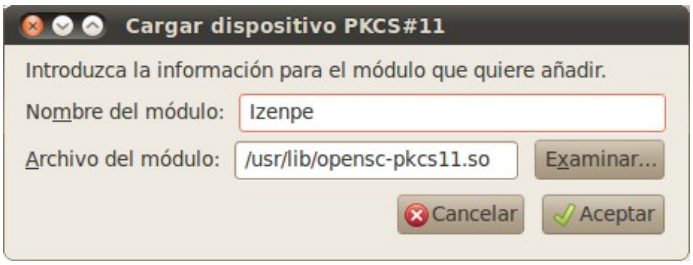
En el menú *Editar → Preferencias* hacemos “click” sobre *Avanzado* y a continuación sobre la pestaña de *Cifrado*, como vemos en la imagen. Por último volvemos a hacer “click” sobre el botón *Dispositivos de seguridad*.

El *Administrador de dispositivos* es una herramienta que permite gestionar los módulos de seguridad de Firefox. Por defecto viene provisto de 2 módulos de seguridad, uno para la gestión de los certificados raíz que vienen preinstalados por defecto y otro para todos aquellos certificados no externos que vayamos añadiendo, junto con las librerías necesarias.

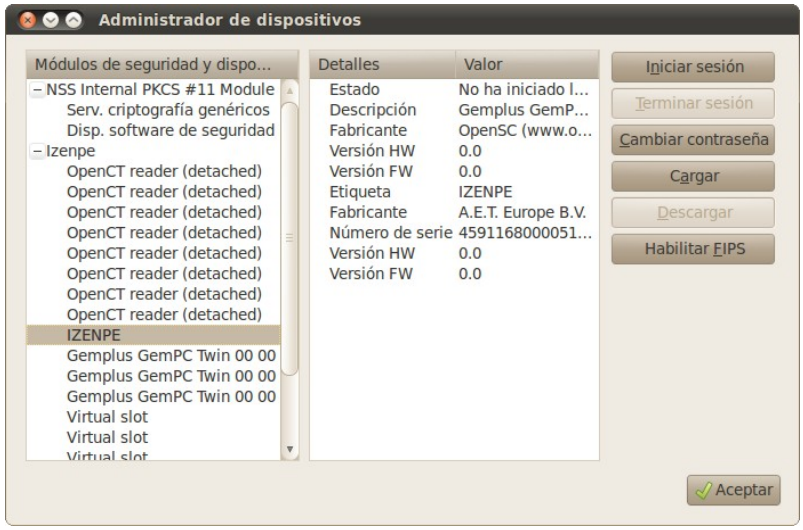
Para añadir el nuevo módulo de seguridad que necesitamos hacemos *"click"* sobre el botón *Cargar*.

Se nos abre una ventana que nos permite definir un nuevo módulo PKCS#11. En este caso nos interesa definir un módulo de integración PKCS#11 con las librerías *opensc*, que solicita la definición de:

- Nombre del módulo: un nombre genérico que haga referencia al módulo de seguridad de las librerías opensc. Introducimos un nombre cualquiera.
- Archivo del módulo: ruta absoluta donde se encuentra el módulo (`/usr/lib/opensc-pkcs11.so`)



Para comprobar que el certificado se ha instalado correctamente debemos comprobar que se ha cargado adecuadamente el nuevo módulo:



Opera

La versión actual de Opera únicamente dispone de soporte para certificados de tipo software (PKCS#12), por lo que no es compatible con los certificados expedidos por Izenpe.

Google Chrome / Chromium

La versión actual de Google Chrome / Chromium no es compatible con los certificados expedidos por Izenpe.

Clientes de correo

Para poder enviar correos firmados es necesario disponer de un certificado que tenga definido como atributo su uso extendido de la clave concretamente la *Protección de correo electrónico (OID 1.3.6.1.5.5.7.3.4).* **Solo algunas de las tarjetas de Izenpe cuentan con dicha extensión**.

Thunderbird

El proceso de configuración de Thunderbird es muy similar al de Firefox.

Instalación de módulo para certificados

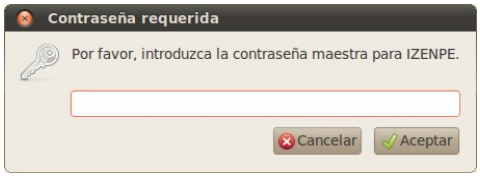
Para la instalación de los certificados y del módulo PKCS#11 ver configuración de Firefox en el apartado correspondiente.

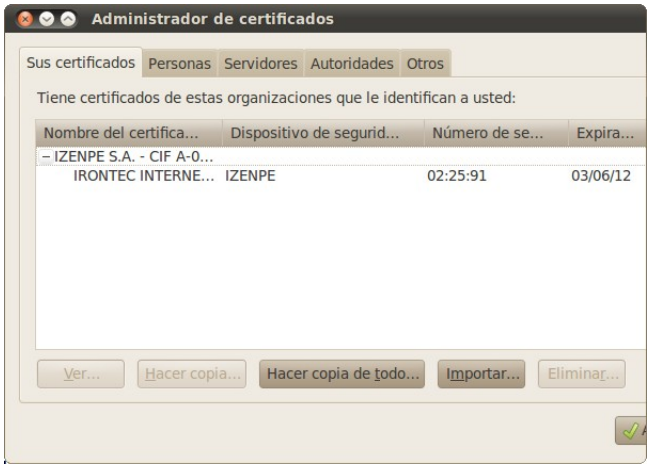
Configuración de cuenta de correo con certificado

La configuración de una cuenta de correo con un certificado correspondiente se muestra en un apartado posterior.

Comprobación

Para comprobar que la carga de certificados se ha realizado correctamente accedemos al menú *Editar → Preferencias → Avanzadas → Certificados → Ver certificados* y seguido nos pedirá el PIN de acceso a la tarjeta





Evolution

Instalación de módulo para certificados

Evolution únicamente soporta de forma nativa certificados software (PKCS#12). Izenpe solo dispone de certificados hardware a través de dispositivos criptográficos. Por ello vamos a tener que hacer una pequeña adaptación del sistema para poder utilizarlo. Evolution puede utilizar las librerías NSS (Network Security Services) de Mozilla, así que enlazaremos el almacén de certificados de Mozilla con el Evolution.

La manera más elegante de realizarlo es a través de una serie de enlaces simbólicos y así tener sincronizadas las configuraciones de los dispositivos de seguridad de Firefox y Evolution (si los copiásemos cada vez que cambiásemos algo tendríamos que volver a copiarlo)

Para ello es necesario abrir una terminal y ejecutar el siguiente comando:

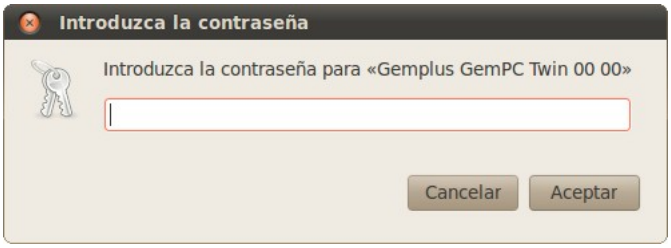
```
$ ln -sf $HOME/.mozilla/firefox/*.default/*.db $HOME/.evolution/
```

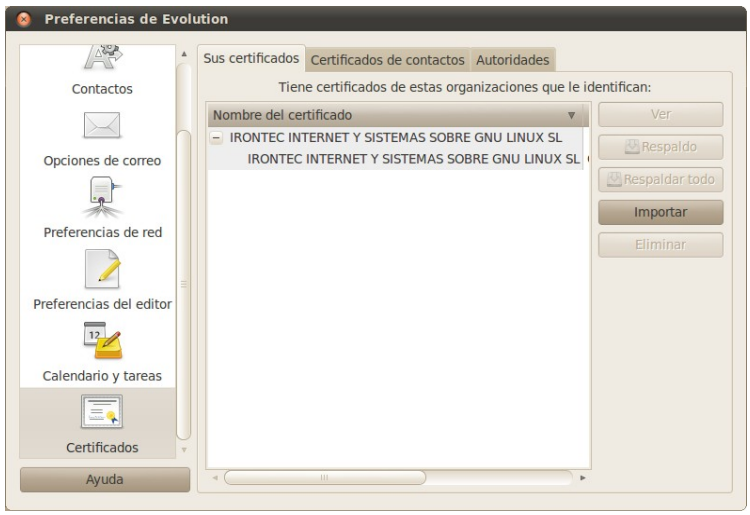
Configuración de cuenta de correo con certificado

La configuración de una cuenta de correo con un certificado correspondiente se muestra en el apartado correspondiente.

Comprobación

Para comprobar que la carga de certificados se ha realizado correctamente accedemos al menú *Editar → Preferencias* y seguido nos pedirá el PIN de acceso a la tarjeta.





KMail

La versión actual de KMail únicamente dispone de soporte para certificados de tipo software (PKCS#12), por lo que no es factible con los certificados expedidos por Izenpe.

Herramientas Ofimáticas

OpenOffice.org

OpenOffice.org no dispone de un gestor de propio de certificados. Aunque es capaz de utilizar el repositorio de certificados de la suite de Mozilla. Por ello **es requerimiento indispensable** para poder firmar documentos ofimáticos con OpenOffice.org **tener previamente configurado** el acceso a certificados digitales a través de Firefox o Thunderbird.

Instalación de certificados de Autoridades de Certificación en aplicaciones

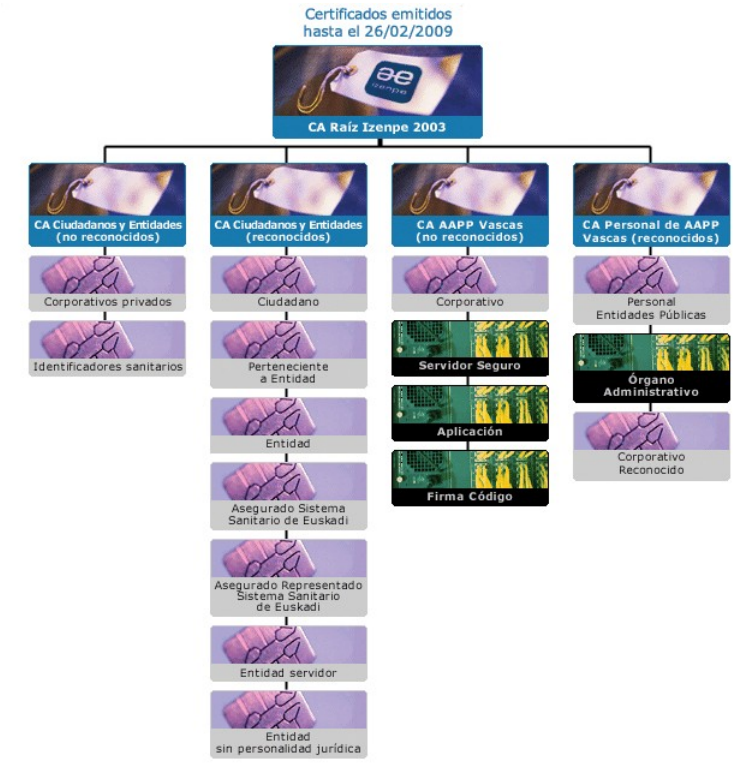
Certificados raíz y subordinados

Izenpe ha dispuesto una jerarquía de autoridades de certificación y subordinadas para dar respuesta a las diferentes necesidades que se presentan al acceder a los diferentes servicios que se proporcionan a través de internet y certifica a sus usuarios con distintos perfiles según el caso.

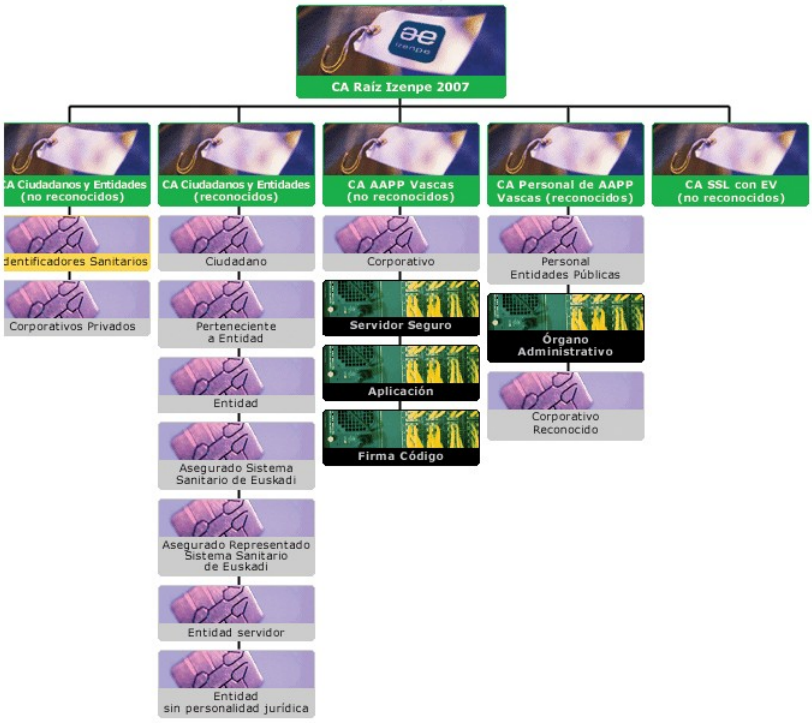
Para una correcta utilización de los certificados digitales en las aplicaciones reales es fundamental la importación de los certificados raíz y subordinados de Izenpe, que podemos encontrar en la web de Izenpe, *www.izenpe.com* → *Descarga de certificados.*

Para descargar los certificados hay que hacer *"click"* sobre las imágenes que tienen dibujada una etiqueta, y **cada etiqueta representa un certificado raíz o subordinado**.

Este esquema pertenece a la **primera jerarquía** de certificación de Izenpe (válido para certificados emitidos por Izenpe antes del 26/02/2009):



Este esquema pertenece a la **nueva jerarquía** de certificación de Izenpe (válido para certificados emitidos por Izenpe a partir del 26/02/2009):



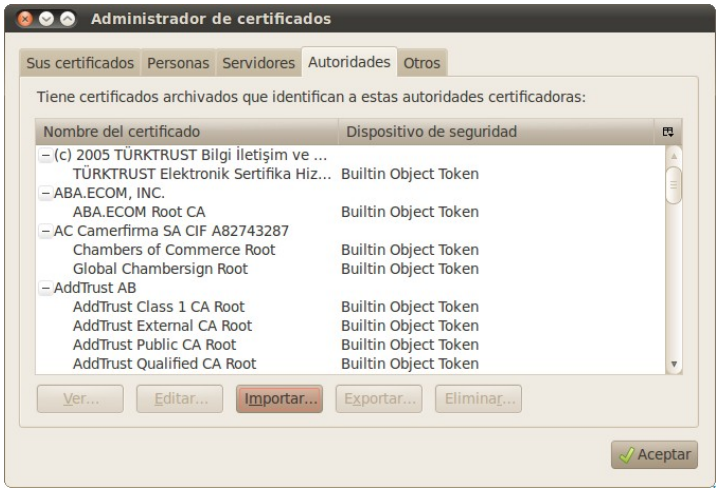
Según la estructura de autoridades certificadoras definidas por Izenpe, cada tarjeta únicamente va a ser validada contra una autoridad raíz y una subordinada. Ello significa que no es estrictamente necesario importar todos los certificados de todas las autoridades certificadoras, ya que el aplicativo en cuestión no va a utilizarlas con nuestra tarjeta. Sin embargo, si no se conoce adecuadamente el funcionamiento de la jerarquía de autoridades **se recomienda instalarlas todas,** tanto las correspondientes a la anterior jerarquía de certificación de Izenpe como a la nueva.

A continuación veremos como instalar los certificados descargados en las distintas aplicaciones:

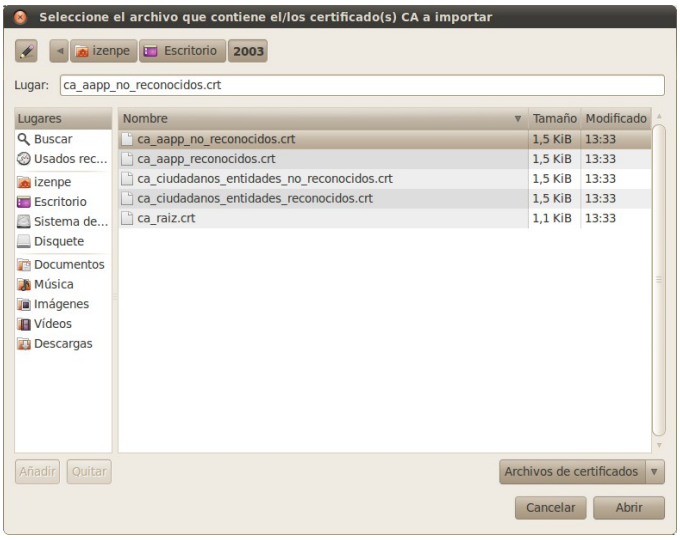
Firefox

Es fundamental importar los certificados raíz de las autoridades certificadoras en Firefox para poder realizar los procesos de autenticación y firma en los sitios web. Si el navegador no dispone de dichos certificados el servidor rechazará el acceso al mismo.

Para importarlos en el menú *Editar → Preferencias* hacemos "click" sobre *Avanzado* y a continuación sobre la pestaña de *Cifrado*. Por último hacemos "click", como se ve en la imagen, sobre el botón *Ver Certificados* y sobre la pestaña *Autoridades* para importar los certificados de las autoridades certificadoras raíz y sus subordinadas.

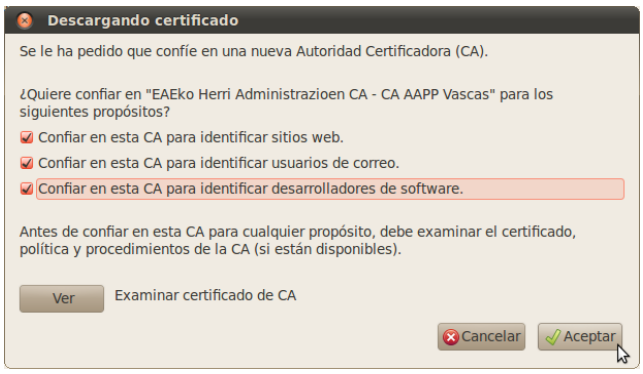


Importamos todos los certificados de las autoridades certificadoras raíz y subordinadas de Izenpe, uno a uno, haciendo "click" en el botón *Importar*:



A la hora de importar los certificados raíz el navegador nos preguntará acerca de la confianza que depositamos sobre el certificado. Existen 3 categorías de confianza:

- Confianza en verificaciones sobre sitios web
- Confianza en verificaciones sobre usuarios de correo
- Confianza en verificaciones sobre desarrolladores de software



Marcamos las 3 categorías.

Este proceso hay que realizarlo para todos y cada uno de los certificados.
Podemos comprobar que aparecen los nuevos certificados:

Thunderbird

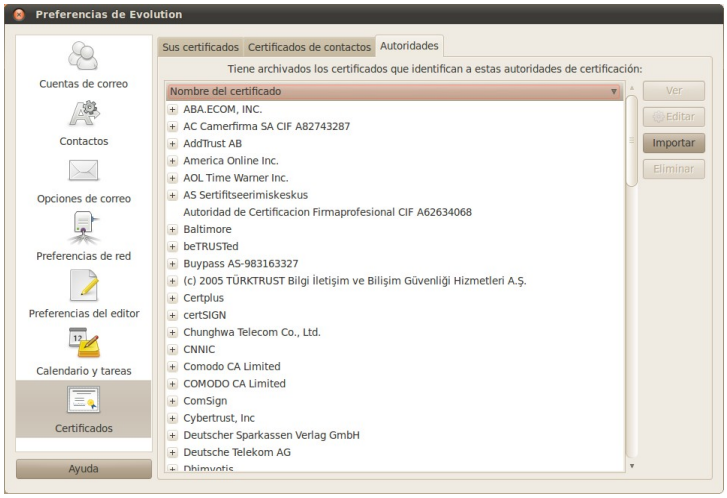
Es importante importar los certificados raíz de las autoridades certificadoras en Thunderbird para poder realizar los procesos de validación de firma sobre los correos. Si el cliente de correo no dispone de dichos certificados no será capaz de garantizar la autenticidad del emisor ni la integridad del correo.

El proceso de configuración de Thunderbird es similar al de Firefox, ver configuración de Firefox en el apartado correspondiente.

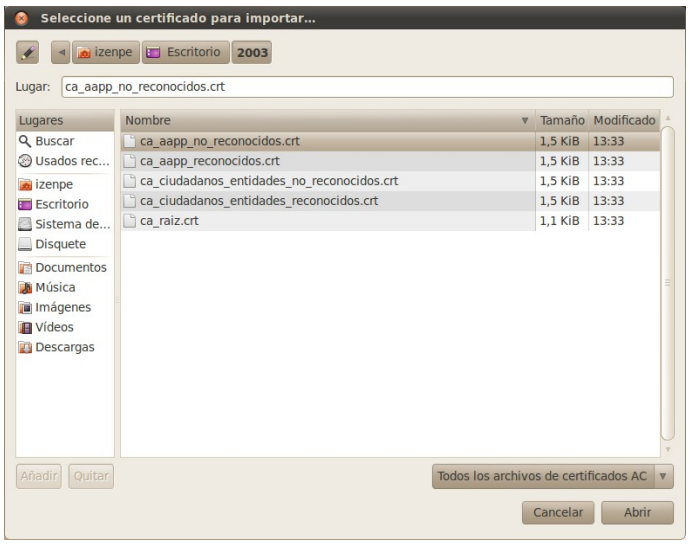
Evolution

Es importante importar los certificados raíz de las autoridades certificadoras en Evolution para poder realizar los procesos de validación de firma sobre los correos. Si el cliente de correo no dispone de dichos certificados no será capaz de garantizar la autenticidad del emisor ni la integridad del correo.

En el menú *Editar → Preferencias* hacemos *"click"* sobre *Certificados* y a continuación sobre la pestaña de *Autoridades*. Hacemos de nuevo *"click"*, sobre el botón *Importar*.

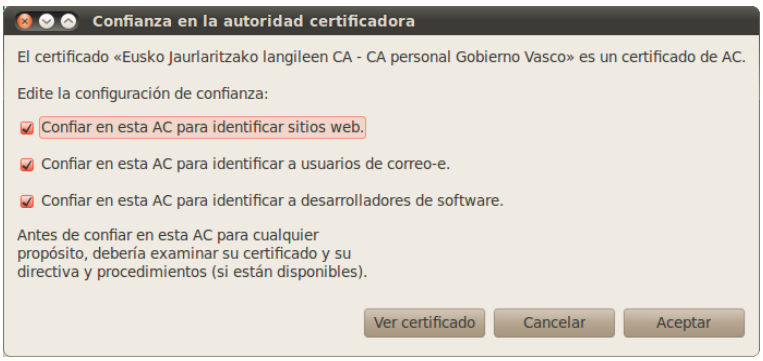


Importamos todos los certificados de las autoridades certificadoras raíz y subordinadas de Izenpe, uno a uno, haciendo *"click"* en el botón *Importar*:



A la hora de importar los certificados raíz el navegador nos preguntará acerca de la confianza que depositamos sobre el certificado. Existen 3 categorías de confianza:

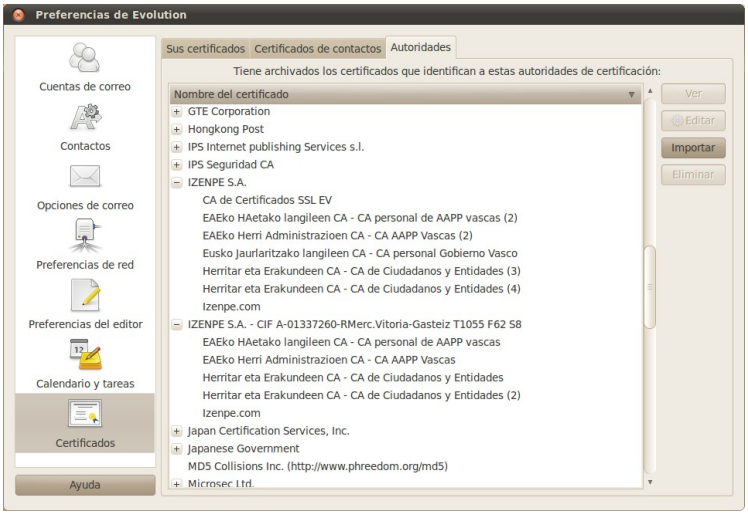
- Confianza en verificaciones sobre sitios web
- Confianza en verificaciones sobre usuarios de correo
- Confianza en verificaciones sobre desarrolladores de software



Marcamos las 3 categorías.

Este proceso hay que realizarlo para todos y cada uno de los certificados de la CA.

Podemos comprobar que aparecen los nuevos certificados:



OpenOffice.org

OpenOffice.org no dispone de gestor de certificados propio y hace uso de los certificados existentes en Firefox o Thunderbird, por lo que la manera de importar certificados raíz de autoridades certificadoras es a través de dichas aplicaciones.

Ejemplo de uso de las aplicaciones

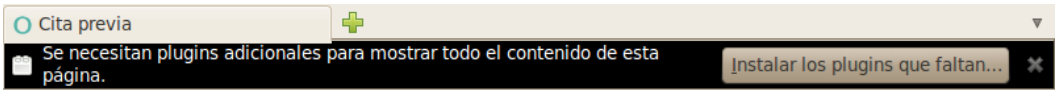
Identificación en sitios web

Firefox

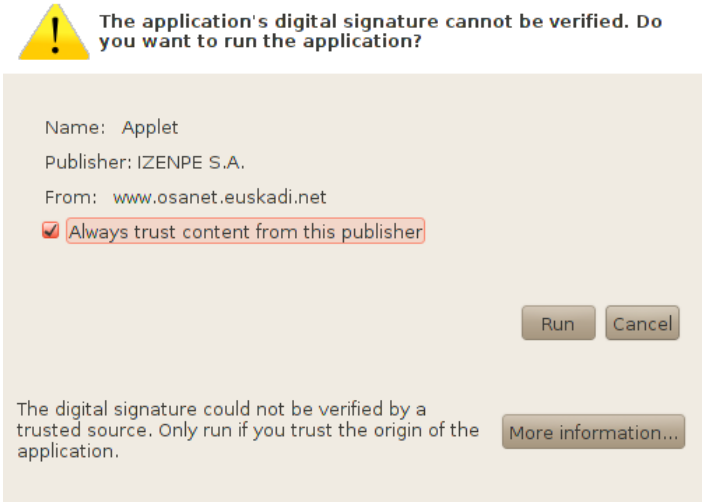
Una vez configurada la ubicación de los certificados según se ha explicado en el apartado correspondiente realizaremos un proceso de autenticación en un sitio web que verifica el acceso al mismo con certificados expedidos por Izenpe: OSANET.

Accedemos al portal de la Sanidad Vasca (http://www.osanet.euskadi.net/), hacemos *"click"* sobre *Reserva tu cita médica* y a continuación en la ventana emergente seleccionamos la opción acceso *mediante tarjeta sanitaria electrónica*.

Para poder acceder al servicio de Osanet, necesitaremos tener el "*plugin"* de Java instalado. Si no lo tenemos, nos aparecerá una advertencia, en la parte superior de la ventana desde donde podremos instalarlo.



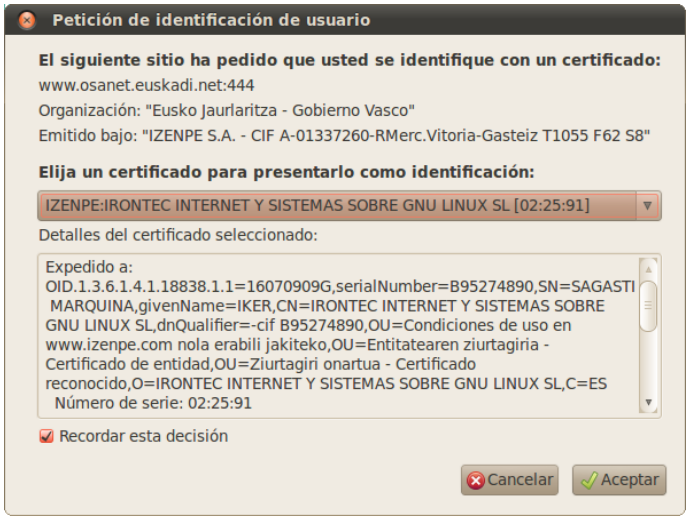
Una vez instalado reiniciamos el navegador, y la primera vez que accedamos, nos aparecerá la siguiente advertencia, en la cual deberemos marcar, que siempre confiaremos y hacer *"click" en "Run".*



Si todo está correctamente configurado se abrirá una nueva ventana solicitando el PIN de la tarjeta de Izenpe.

Nota: La primera vez que accedamos a OSANET, nos aparecerá una advertencia relacionada con permitir o no permitir las ventanas emergentes. En este caso, permitiremos la ventanas emergente.

Introducimos correctamente el PIN y nos mostrará una nueva ventana permitiéndonos seleccionar con cual de todos los certificados instalados en el servidor queremos autenticarnos. Seleccionamos el certificado de Izenpe y hacemos *"click"* sobre *Aceptar*.



Si nuestro certificado es válido para acceder a la aplicación y no está revocado la aplicación nos permitirá el acceso con las mismas garantías que lo hacemos de forma presencial.

Nota: Es importante que cuando acabemos de realizar las gestiones oportunas cerremos la sesión del sitio web así como el navegador para evitar que otras personas puedan acceder a Internet con nuestros credenciales.

Envío de correos firmados digitalmente

Tal y como hemos comentado anteriormente para poder enviar correos firmados es necesario disponer de un certificado que tenga definido como atributo su uso extendido y solo algunos de los certificados de Izenpe cuentan con dicha extensión.

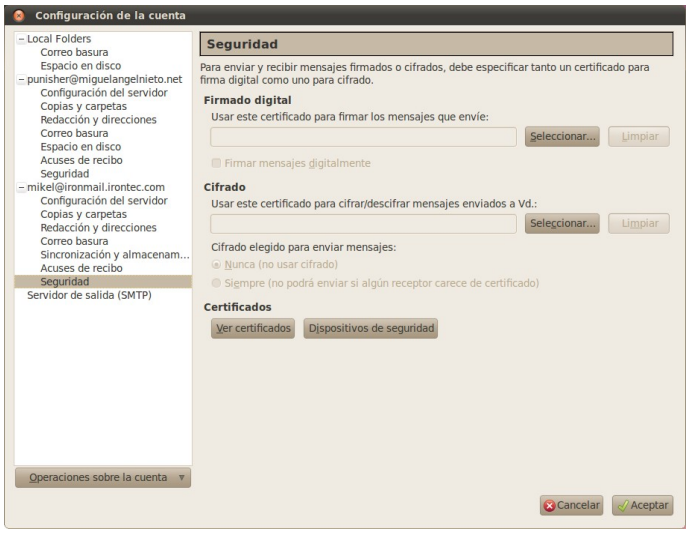
Una vez dispongamos de un certificado válido, será necesario asociar la cuenta de correo con el certificado en cuestión. Esta cuenta de correo debe ser la misma que la incorporada en el certificado.

Veamos como realizar dicha tarea en los distintos clientes de correo.

Thunderbird

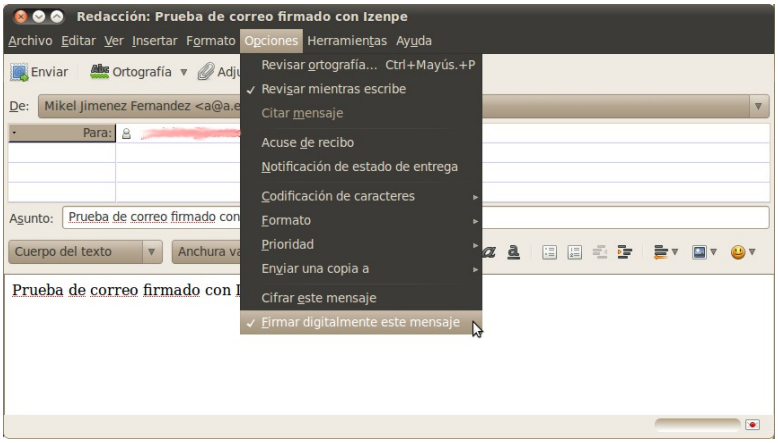
Configuración cuenta de correo con certificado

En el menú *Editar* → *Configuración de las cuentas* hacemos “click” sobre el apartado de *Seguridad* en la cuenta correspondiente. A continuación seleccionamos el certificado



Envío de correo firmado digitalmente

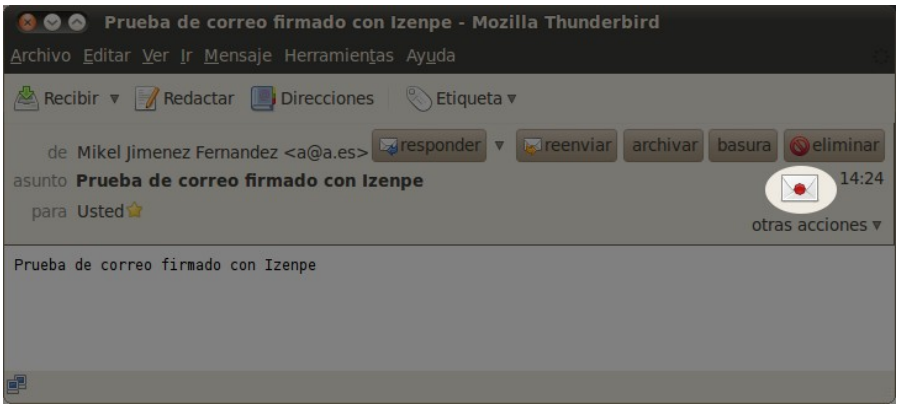
Para enviar un correo firmado digitalmente es necesario indicarlo. Si no tenemos marcada la opción de firmar digitalmente todos los correos salientes, podemos hacerlo manualmente a través del menú *Opciones → Seguridad → Firmar digitalmente este mensaje.*



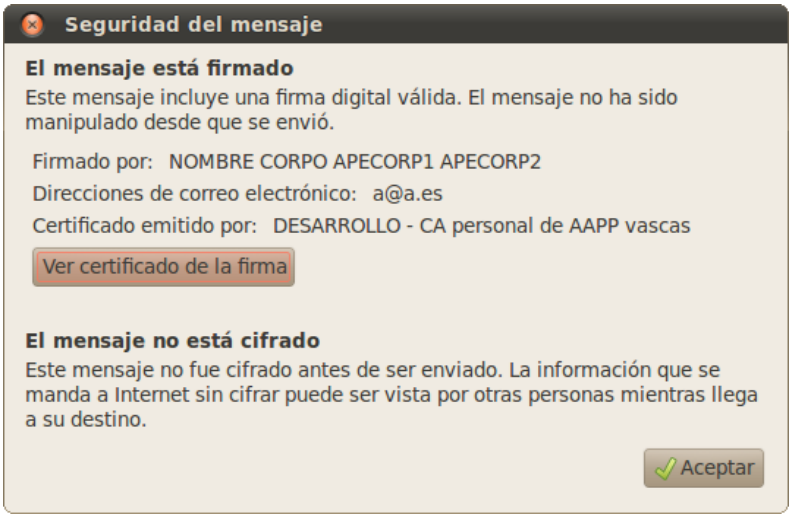
Observaremos en la parte inferior de la ventana de redacción de correo un icono que indica que hemos seleccionado la opción de firmar el correo digitalmente.

Verificación de firma digital en correo

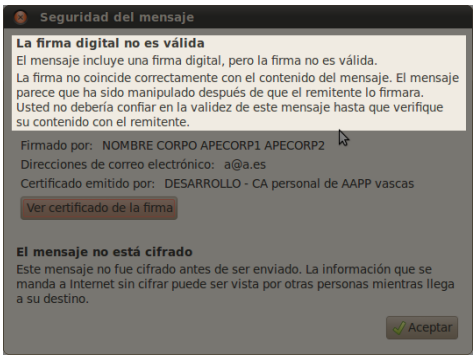
Thunderbird nos muestra un icono que indica que el correo está firmado digitalmente.

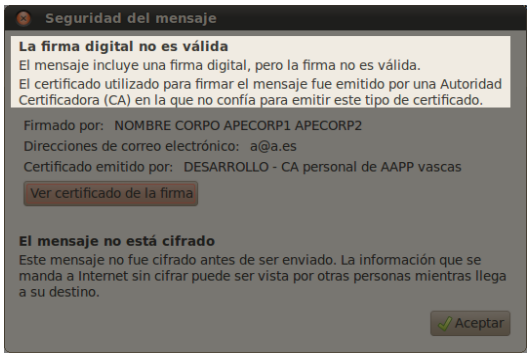


Para poder comprobar si la firma es válida **es necesario haber importado los certificados raiz de las autoridades certificadoras y subordinadas**.



En caso que no sea válida nos avisará de ello. Bien porque el correo ha sido modificado o bien porque no hemos importado los certificados raíz de las autoridades certificadoras y sus subordinadas.

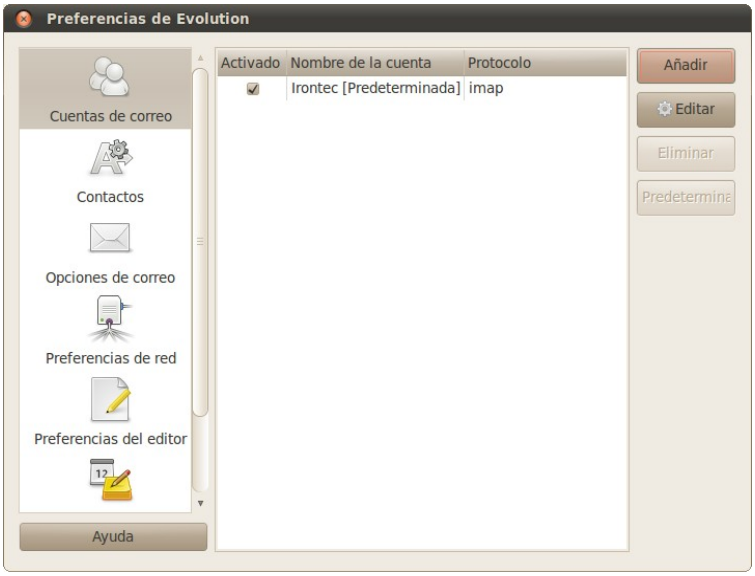




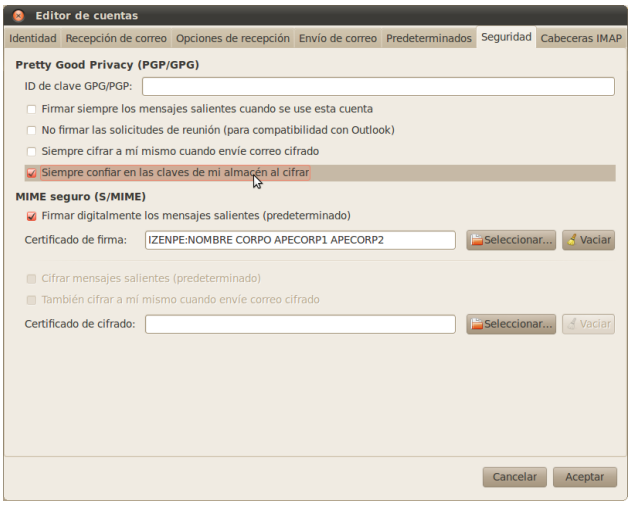
Evolution

Configuración cuenta de correo con certificado

En el menú *Editar* → *Preferencias* hacemos “click” sobre la opción *Cuentas de correo*, seleccionamos la cuenta que queremos configurar y volvemos a hacer “click” en *Editar*.

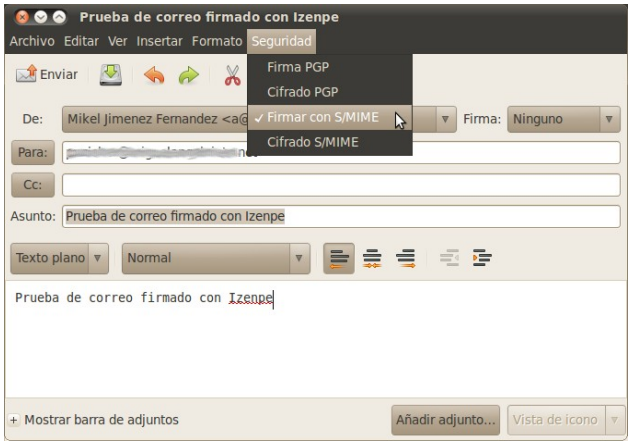


Accedemos a la sección *Seguridad* y seleccionamos el certificado que queremos utilizar para la firma de correos haciendo “click” en el botón *Seleccionar* del apartado *MIME Seguro*.



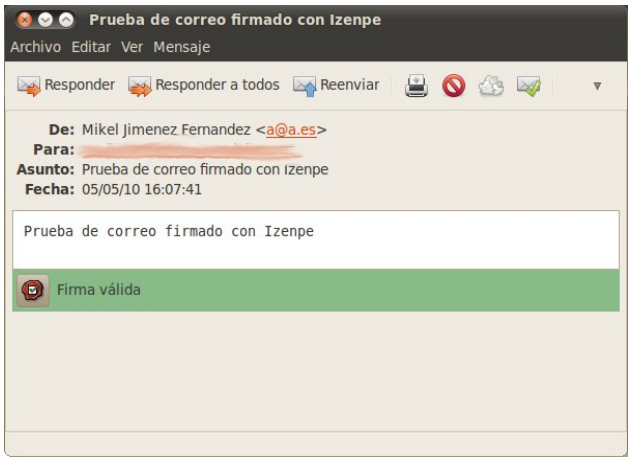
Envío de correo firmado digitalmente

Para enviar un correo firmado digitalmente es necesario indicarlo. Si no tenemos marcada la opción de firmar digitalmente todos los correos salientes, podemos hacerlo manualmente a través del menú *Seguridad → Firmar con S/MIME.*



Verificación de firma digital en correo

Evolution nos muestra un icono que indica que el correo está firmado digitalmente.



Para poder comprobar si la firma es válida **es necesario haber importado los certificados raiz de las autoridades certificadoras y subordinadas**.

Firma de documentos ofimáticos

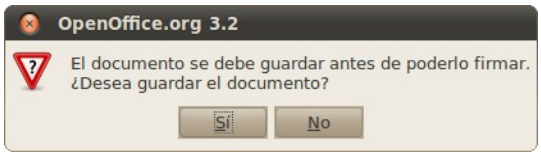
OpenOffice.org

Una vez configurada la ubicación de los certificados según se ha explicado en el apartado correspondiente realizaremos un proceso de firma de un documento ofimático.

OpenOffice.org permite firmar los siguientes tipos de documentos:

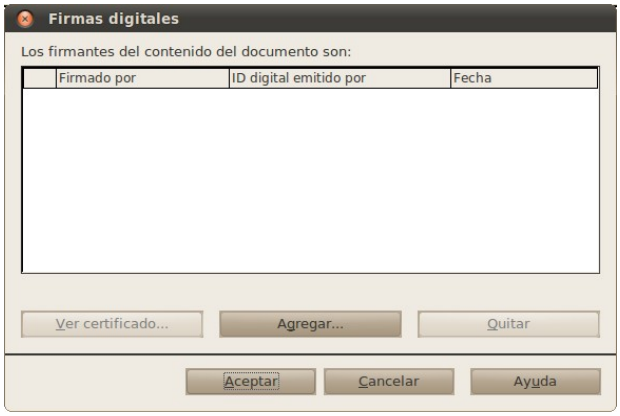
- Documentos de texto (OOWriter)
- Hojas de cálculo (OOCalc)
- Presentaciones (OOImpress)
- Dibujos (OODraw)

Para proceder con la firma del documento, en el menú *Archivo* seleccionamos la opción *Firmas digitales.*

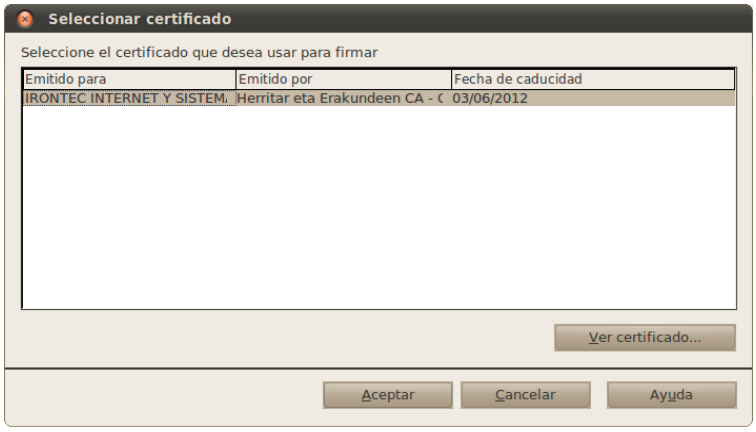


La firma del documento es necesario realizarla sobre un documento guardado, que no se va a modificar. En el momento en que se firma el documento si se modifica se pierde la firma y es necesario volver a firmarlo.

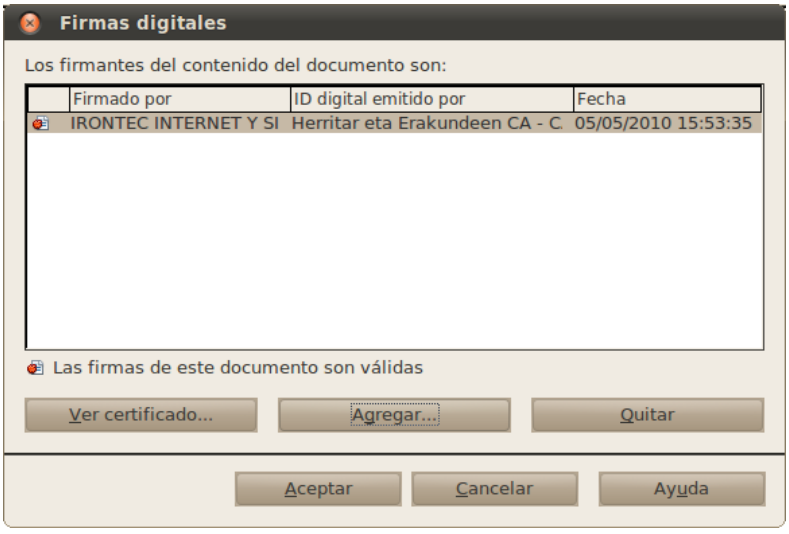
Una vez guardado nos muestra el gestor de firmas digitales de OpenOffice.org



Hacemos “click” sobre *Agregar* y nos muestra los certificados que tenemos configurados desde la base de datos de certificados referenciada (Firefox)

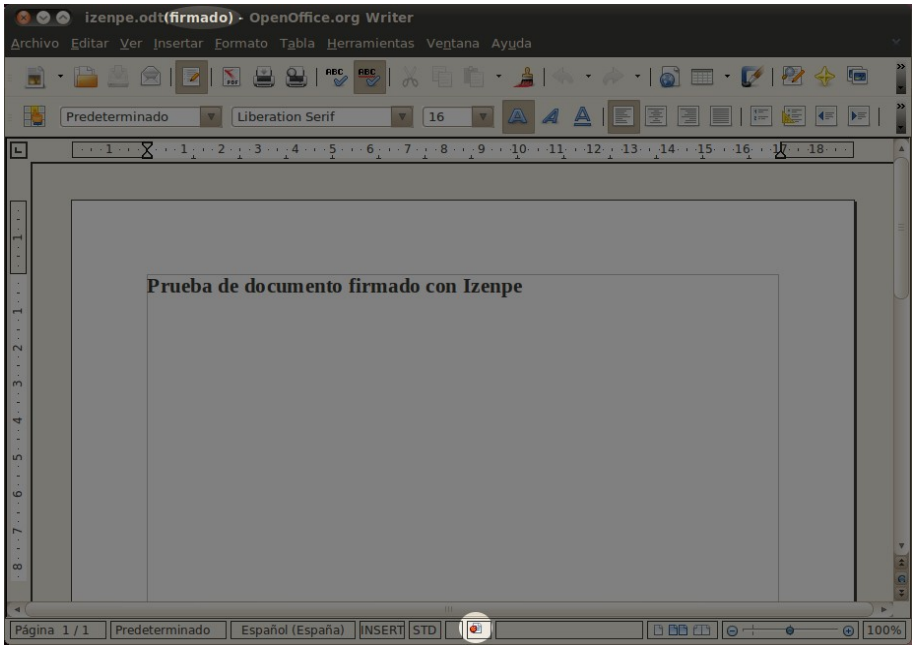


En la ventana que se abre nos aparecerán tantos certificados como tengamos configurados. Seleccionamos el certificado en cuestión y pulsamos sobre *Aceptar*.



Para que las firmas del documento sean válidas es necesario tener importadas los certificados de las autoridades raíz y subordinadas correspondientes. Pulsamos sobre *Aceptar* de nuevo y ya tenemos el documento firmado.

Podemos distinguir dos elementos distintivos que nos indican la existencia una o más firmas sobre el documento:



Otras aplicaciones adicionales

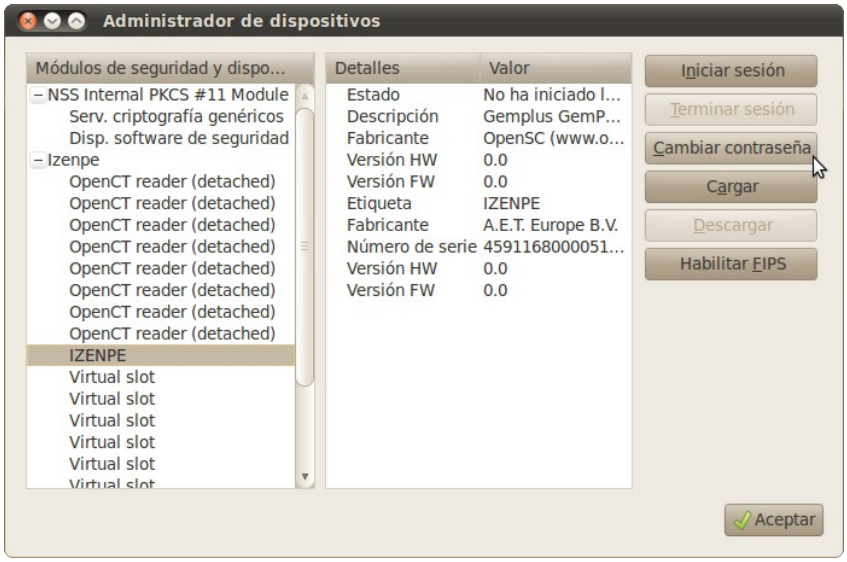
Cambio de PIN

El PIN es un sistema de cifrado simétrico utilizado para garantizar la seguridad del certificado alojado en la tarjeta, en caso de pérdida o de uso no autorizado. Para poder cambiar el PIN es necesario conocer el PIN actual. Además la tarjeta no debe estar bloqueada por haber fallado 3 o más intentos seguidos de introducir el PIN.

Las tarjetas de Izenpe permiten definir un PIN entre 4 y 8 caracteres alfanuméricos (a-z, A-Z, 0-9).

De forma gráfica, a través de Firefox

En el menú *Editar* → *Preferencias* pinchamos sobre *Avanzado* y a continuación sobre la pestaña de *Cifrado*, como vemos en la imagen. Por último pinchamos sobre el botón *Dispositivos de seguridad* y seguido a *Cambiar contraseña*



Nos aparecerá una ventana que nos permite cambiar el PIN, previa introducción del PIN actual.

A través de la línea de comandos

Abrimos una terminal de línea de comandos y en modo superusuario ejecutamos los siguientes comandos:

```
# apt-get install opensc
# pkcs11-tool --change-pin

Please enter the current PIN:
Please enter the new PIN:
Please enter the new PIN again:
PIN successfully changed
```

Desbloqueo de PIN

Actualmente esta funcionalidad no está soportada por las tarjetas de Izenpe para las plataformas GNU/Linux.

Créditos

Este documento ha sido elaborado conjuntamente por las empresas Irontec Internet y Sistemas sobre GNU/Linux y zylk.net.

Para la elaboración del presente documento se ha desarrollado una cuidadosa metodología de análisis y puesta en funcionamiento, garantizado la adecuación del documento a las necesidades de los usuarios.

Si el lector considera que hay algún aspecto erróneo o encuentra alguna errata, puede trasladarla mediante email a cau-izenpe@izenpe.net e intentaremos incluirla en próximas revisiones del documento.