Manual de Instalación
Certificado Digital Izenpe

Windows
Windows 8

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

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

Índice 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 13.04 LTS 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 y Alcance 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 Windows:

- Requisitos de Hardware (Lectores) y Software (Aplicaciones externas).
- Descarga e Instalación del Middleware de Izenpe.
- Descarga e Instalación de los certificados para Izenpe.
- Configuración y ejemplos de uso para las distintas aplicaciones soportadas.
- Errores conocidos, consejos y soluciones.

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

Este documento pretende servir de manual de instalación para Windows 8 y posteriores.

Hardware y Aplicaciones Soportadas

Algunos De Los Lectores Soportados

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:

- miniLector USB
- Cherry Keyboard
- miniLector BAY
- miniLector PCMCIA-92

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.

Nota Importante: El lector de tarjetas ha de ser compatible PC/SC.

Tarjetas Inteligentes Soportadas De Forma Nativa

El Universal Middleware de Izenpe para Linux (en adelante UM) consiste en un módulo de librería que expone una API compatible con la especificación PKCS#11 v2.11.

Dicho módulo ofrece al software que utilizan las diversas interfaces de programación la posibilidad de utilizar las tarjetas inteligentes soportadas como tokens criptográficos.

La siguiente lista consta de las tarjetas que son compatibles con el módulo de Izenpe.

- Gemalto Classic TPC:
  - FileSystem full compliant PKCS#11 con objetos de 2048 bit
  - FileSystem de Firma electrónica con validez legal con objetos de 2048 bit
- Giesecke&Devrient (StarCOS 2.3)
  - FileSystem full compliant PKCS#11 con objetos de 1024 bit
- Incard Incrypto34 V2 con filesystem: CNS + Firma electrónica + FullP11:
  - FileSystem CNS conforme a las especificaciones CNS del CNIPA (v.1.1.3) (FS CNS)
  - FileSystem de Firma electrónica con validez legal (FS DS-v1.0)
  - FileSystem full compliant PKCS#11 (FS FullP11)
- Incard Touch&Sign2048:
  - Todos los filesystem soportados en la tarjeta Incrypto34v2 más:
    - FileSystem full compliant PKCS#11 (FS FullP11), con objetos de 2048 bit
    - FileSystem de Firma electrónica reconocida (FS DS-v2.0), con tres pares de claves de 2048bit o con tres pares de claves de 1024bit más tres pares de claves de 2048bit.

Tarjetas Inteligentes Soportadas Mediante El Uso De Librerías PKCS#11 Externas:

- Incard CryptoSmartCard16 (SetecOS)
- Incard CryptoSmartCardE4H (Starcos)
- Incard M4.01a FS1111 (Siemens CardOS/M4)
- Gemplus (GemGATE 32K)
- Gemplus (GemGATE CardOS M4)
- Siemens (Siemens CardOS M4.01)
- Siemens (Siemens CardOS M4)
- Siemens (Siemens CIE)
- Siemens (Siemens SISS – HPC)
- Siemens (Siemens CardOS M4.01a)
- Athena (ASECard Crypto)
- Ghirlanda (M4cvToken)
- Gemplus (SIM TIM)
- Oberthur (Cosmo 64 RSA dual interface)
- Oberthur (Oberthur Cosmo64).

Aplicaciones Soportadas

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 24.0
  - Google Chrome / Chromium 31.0.1650.57

- Herramientas Ofimáticas
  - LibreOffice 3.5.4.7

Requisitos Software para la Instalación

Configuración de los lectores

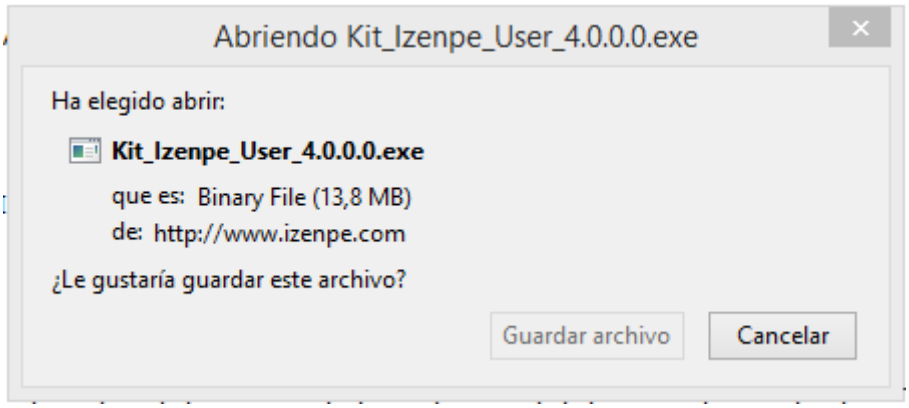
En las ultimas versión de Windows como 7 y 8 los drivers o controladores de nuestro lector de tarjetas inteligentes se instalaran solos.
Para versiones algo mas antiguas como Windows XP tendremos que buscar los drivers específicos para nuestro lector en la pagina del fabricante del mismo.

Descarga e Instalación del Middleware de Izenpe

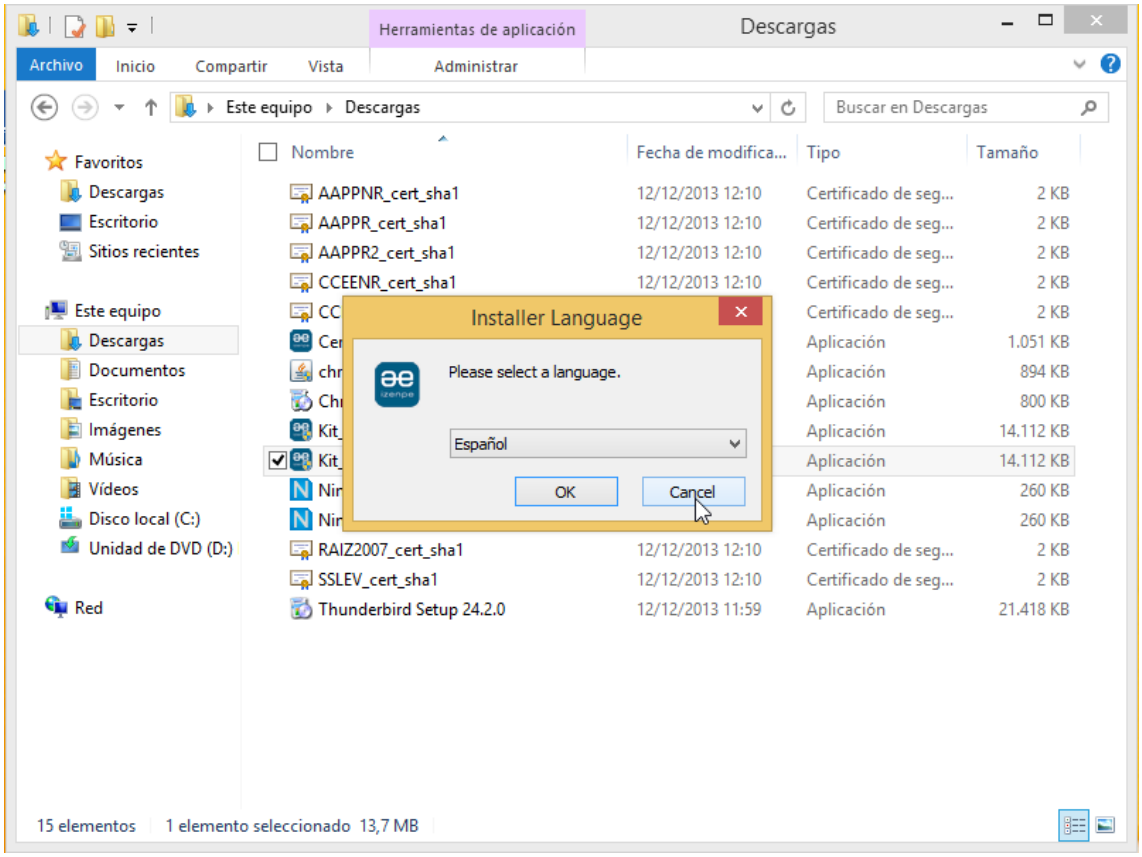
Para la descarga del Middleware, iremos a la web de izenpe y en el apartado *Software* encontraremos para descargar el archivo que nos interesa.

www.izenpe.com

En nuestro caso seleccionaremos Windows y haremos click en “Software de izenpe”



Guardaremos el archivo y posteriormente lo ejecutamos haciendo click derecho sobre el archivo descargado y seleccionando la opción “Ejecutar como Administrador”

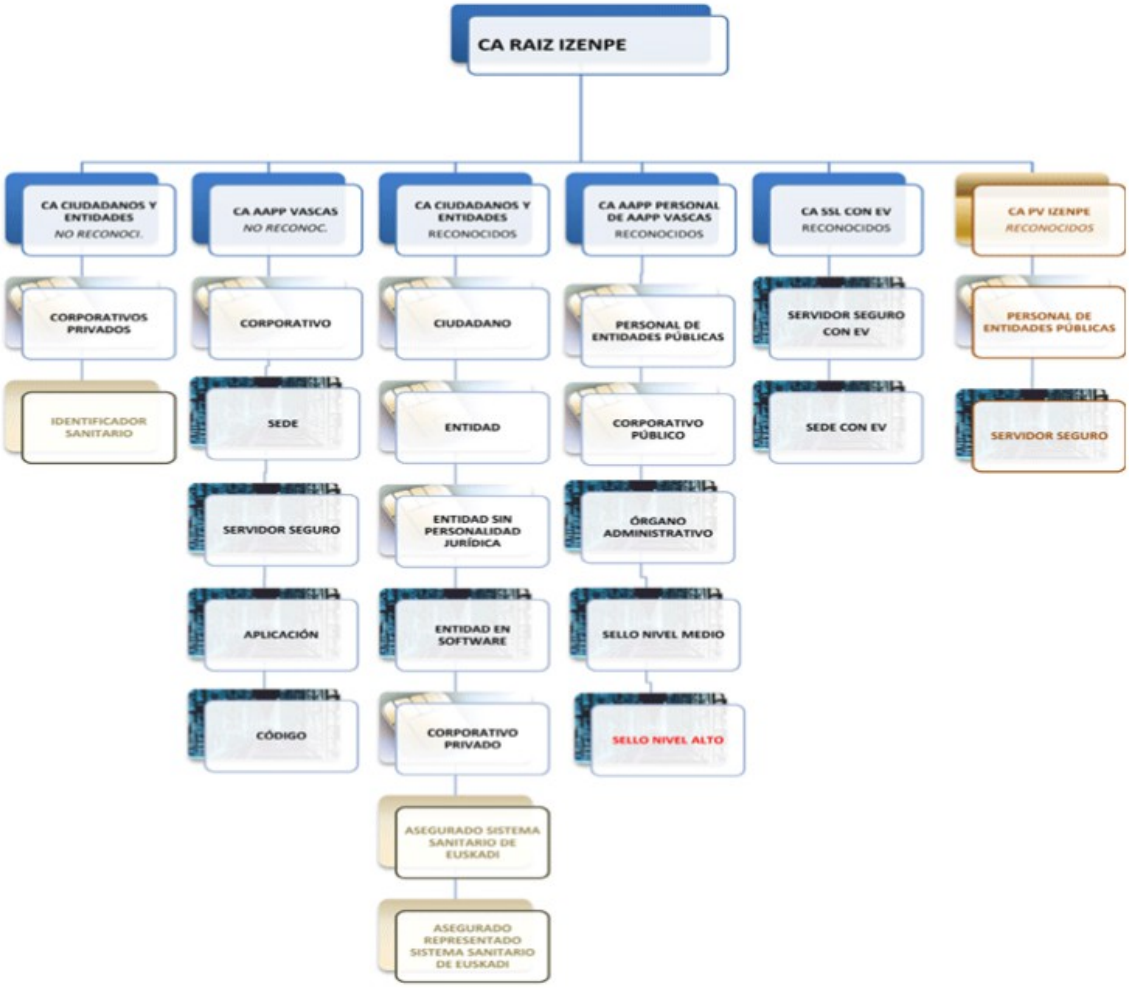


Nota: *El sistema necesitara reiniciarse tras la instalación, por lo tanto guardar todo previamente..*

Seguir los pasos que nos dicte el asistente para completar la instalación, hasta que no se reinicie el sistema no se completara.

Descarga e Instalación de los Certificados Izenpe

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 ver el gráfico mas grande: https://servicios.izenpe.com/images/CAS-IZENPE-2011.gif

Forma 1 – Modo Automático

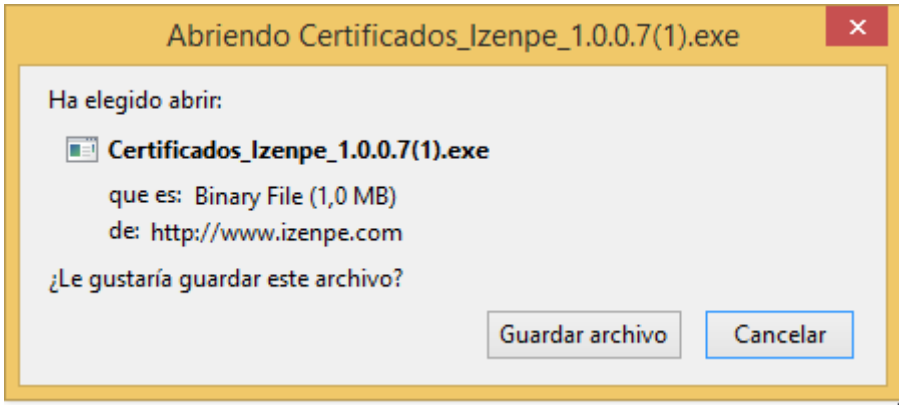
Izenpe ha desarrollado una serie de instaladores especiales para cada plataforma, cuyo objetivo es conseguir que la descarga e instalación de los certificados no sea tan compleja como solía ser por las características del software vigentes hasta la fecha.

En este caso el instalador que nos interesa es un paquete **.deb**, compatible para las distribuciones que usan este tipo de paquetes, como son Ubuntu, Debian, Linux Mint ...

Para la descarga de los certificados, iremos a la web de izenpe y en el apartado *Software* encontraremos el archivo para su descarga.

www.izenpe.com

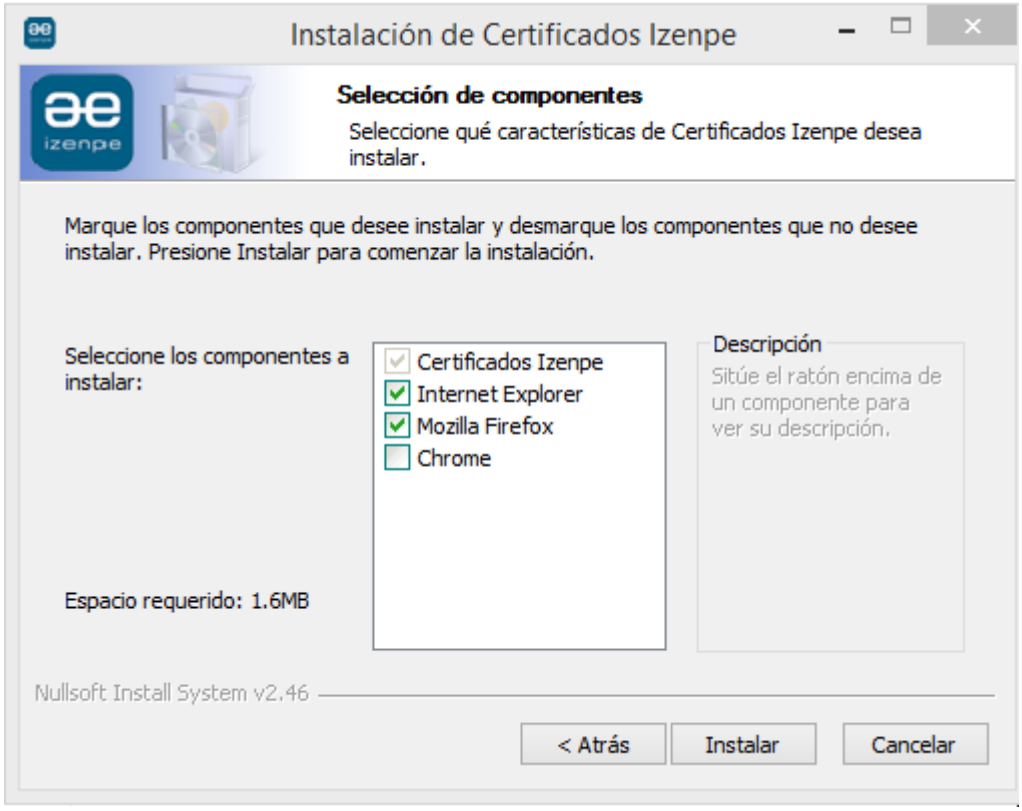
Seleccionamos *Certificado Izenpe para Windows* y le damos a *Guardar Archivo*.



Nota: *Por defecto se guardará en la carpeta descargas dentro de tu directorio personal.*

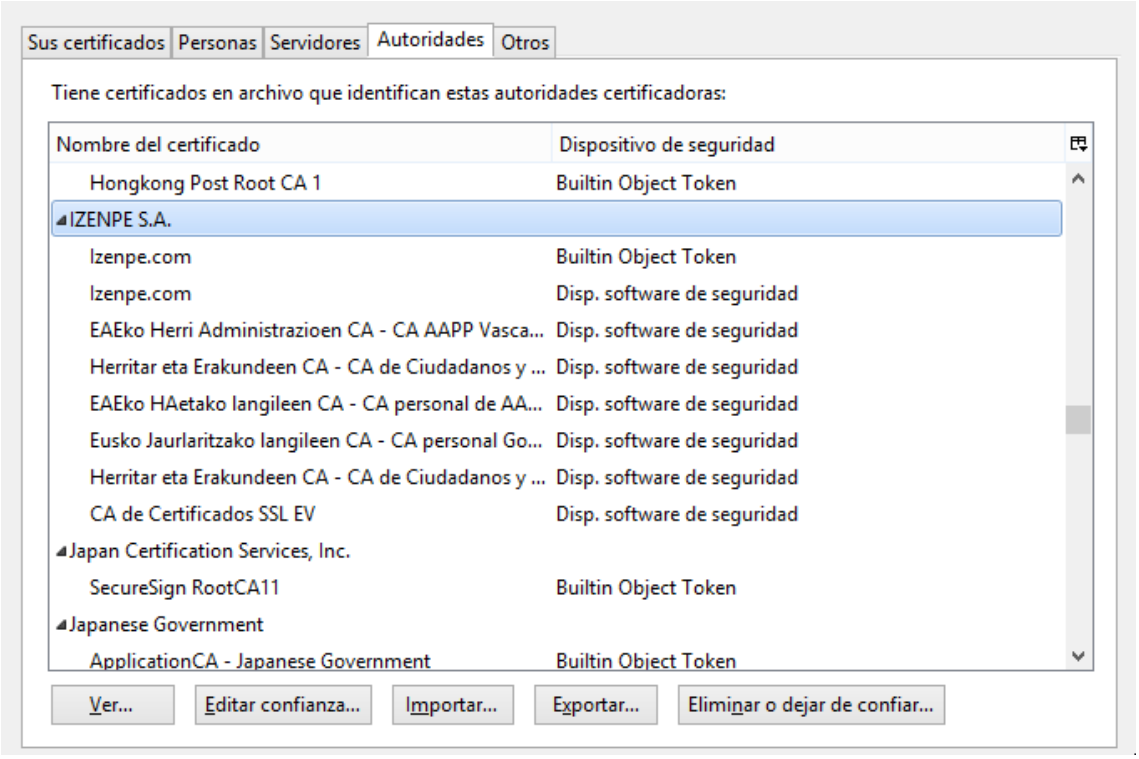
Una vez finalizada la descarga ejecutamos el archivo descargado de la misma manera que lo hicimos anteriormente con el middleware.

Seguimos el asistente y seleccionamos los navegadores con los que queramos trabajar



Si se desea se puede comprobar si la instalación ha sido exitosa consultando los certificados instalados en tu navegador.

Ruta: Firefox → Opciones → Opciones → Avanzado → Certificados → Ver certificados → Autoridades; Aquí buscando por Izenpe deberíamos tener ocho entradas.



Nota: Si tenemos también instalado el navegador Chrome en nuestro equipo, y desea configurarlo, puede seleccionarlo y se importaran los certificados en su base de datos.

Forma 2 – Modo Manual

Si el paso anterior no esta disponible por algún motivo, siempre podemos realizar la descarga e instalación de cada certificado a mano. Un proceso bastante costoso.

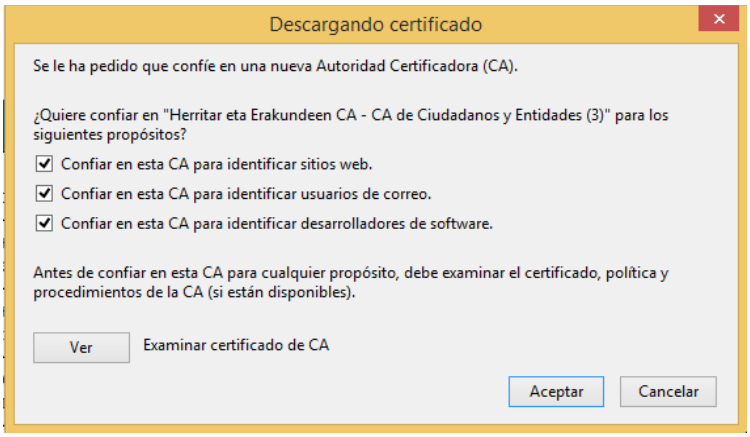
Estos certificados, están disponibles en la web: www.izenpe.com → Descarga de certificados.

Enlace Directo a los certificados→ https://servicios.izenpe.com/jsp/descarga_ca/descarga.htm

HUELLAS DIGITALES CA RAÍZ 2007			
SHA1		SHA2	
CA Raíz de Izenpe 2007 [30 77 9E 93 15 02 2E 94 85 6A 3F F8 BC F8 15 B0 82 F9 AE FD]		**CA Raíz de Izenpe 2007** [2F 78 3D 25 52 18 A7 4A 65 39 71 B5 2C A2 9C 45 15 6F E9 19]	
Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3) [06 FB AC 35 AE 18 FC BF 22 29 78 8D D1 2D AC 89 8E 74 52 AE]		**Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3)** [87 56 60 A3 5C B1 03 D7 E0 BB 00 44 24 F1 6D BF BF 21 E0 B4]	
Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) [9F DC E9 42 9B 3D 7E 59 49 9D C3 F8 3C 93 66 65 22 69 A7 59]		**Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)** [08 D8 D6 2A 1A 15 36 C5 3A 0F 9A 18 35 BF 82 C9 F0 96 83 23]	
EAEko Herri Administrazioen CA - CA AAPP Vascas (2) [7F 58 BB 8F 87 11 C0 49 61 28 CF 71 63 4B 77 95 0A DD D3 2C]		**EAEko Herri Administrazioen CA - CA AAPP Vascas (2)** [F7 9C DA 11 E7 91 74 19 A0 41 8D B8 4B A7 43 C5 31 3A D7 F0]	
EAEko HAetako langileen CA - CA personal de AAPP vascas (2) [E5 C8 62 ED DC F1 14 C8 26 61 98 4A D6 48 AD F2 3F 51 10 FC]		**EAEko HAetako langileen CA - CA personal de AAPP vascas (2)** [93 A1 44 6B 61 99 4B 5B 0E 99 D0 5B 14 CD BB 32 2E 6C 17 64]	
CA de Certificados SSL EV [67 16 29 9C C4 C0 CA 25 52 EE 88 01 9A FC EE 49 B2 A1 63 34]		**CA de Certificados SSL EV** [6C 48 4D 0F 4D B2 95 EC 67 EB B3 E0 5E 3D C2 14 49 2A 9A B8]	
Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco [4A 17 ED D4 9E D4 CC 39 24 3A BE 74 B8 92 DF AA 00 68 6A 80]		**Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco** [25 E9 D1 6D F8 D6 4A 60 73 40 8C BE 24 8E 52 9C 23 9E 32 92]	

HUELLAS DIGITALES CA RAÍZ 2003 SHA1	
CA Raíz de Izenpe 2003 [4A 3F 8D 6B DC 0E 1E CF CD 72 E3 77 DE F2 D7 FF 92 C1 9B C7]	
Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (2) [42 80 FD 5F 9A 4B 79 68 A2 A0 54 E3 2A 18 30 D4 06 BA 94 05]	
Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades [B9 CA B0 0E 41 38 06 AA 3F EA 3A 5B 28 F9 BB 39 E7 EF 15 0A]	
EAEko Herri Administrazioen CA - CA AAPP Vascas [7B 11 62 CC 37 DC 3D 43 DB EF 46 B9 D6 05 FB 6F 93 F2 18 38]	
EAEko HAetako langileen CA - CA personal de AAPP vascas [85 6B EE 62 FC 8E 99 B9 A6 5C 15 29 02 09 BE F9 87 ED E4 E4]	

Para descargar los certificados hay que hacer *"click"* sobre las imágenes que tienen dibujada una flecha blanca en un recuadro azul. No saldra una ventana como esta en la que debemos seleccionar todas las ociones.



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.**

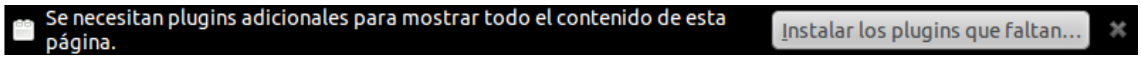
Es fundamental importar los certificados raíz de las autoridades certificadoras en Firefox para poder realizar los procesos de autenticación y firma en los sitios web. Si el navegador no dispone de dichos certificados el servidor rechazará el acceso al mismo.

Para comprobar si hemos importado bien los diferentes certificados podremos ejecutar los mismos pasos realizados anteriormente.

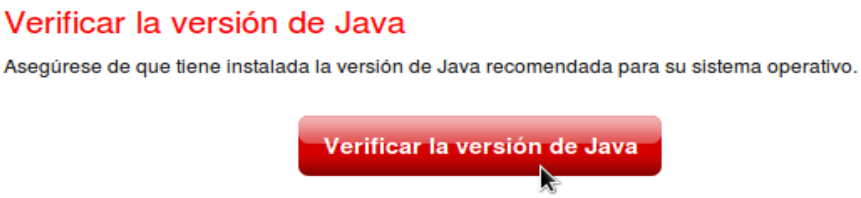
Descarga e Instalación de JAVA JRE de Oracle

Para que funcione correctamente el Applet que gestiona la conexión a las webs y la firma de documentos online (Applet de Idazki), es necesario tener instalada en el equipo la última versión de **Java JRE de Oracle**.

Si no lo esta, es posible que nos encontremos con algo como esto al entrar en las webs, y la instalación automática suele fallar o está casi siempre desactivada:



Para comprobar si tenemos la ultima versión: http://www.java.com/es/download/installed.jsp



Si no fuera este el caso, descargaremos la última versión.

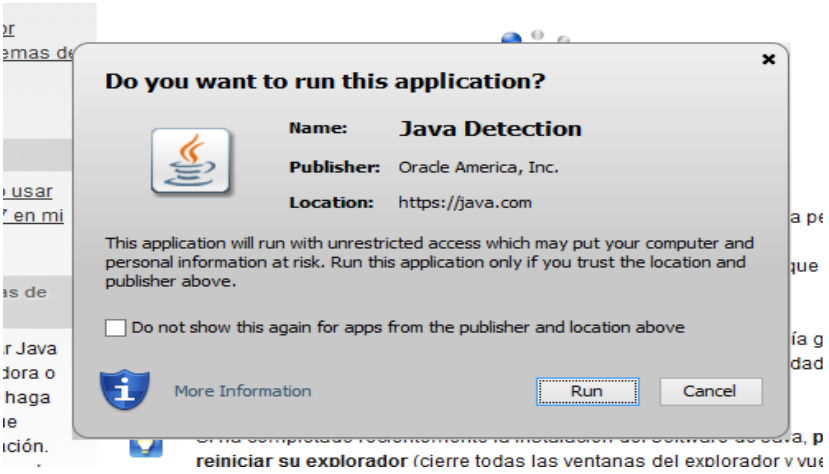
No nos hace falta determinar si nuestro sistema es de 64b o de 32b, esto lo hace automáticamente la web y descarga la versión a corde a nuestra arquitectura.

· Cuando finalice la descarga, cerramos Firefox.

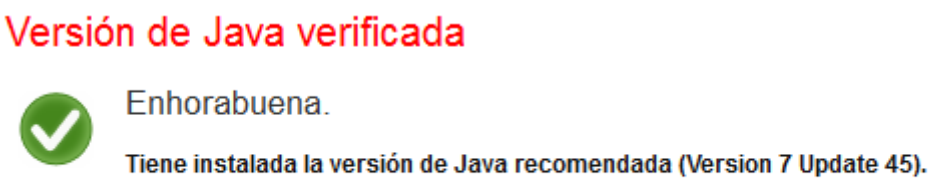
· Ejecutamos el archivo descargado previamente (cerrar todos los navegadores).

Para comprobar si la instalacion se ha realizado correctamente abriremos un navegador e iremos de nuevo a la pagina oficial de java: http://www.java.com/es/download/installed.jsp

Nos saldrá una ventana que nos avisa de una vulnerabilidad al permitir la ejecución de java debemos permitirla.



Si hemos hecho la instalación correctamente deberíamos ver una pantalla similar a esta:



Configuración de las aplicaciones

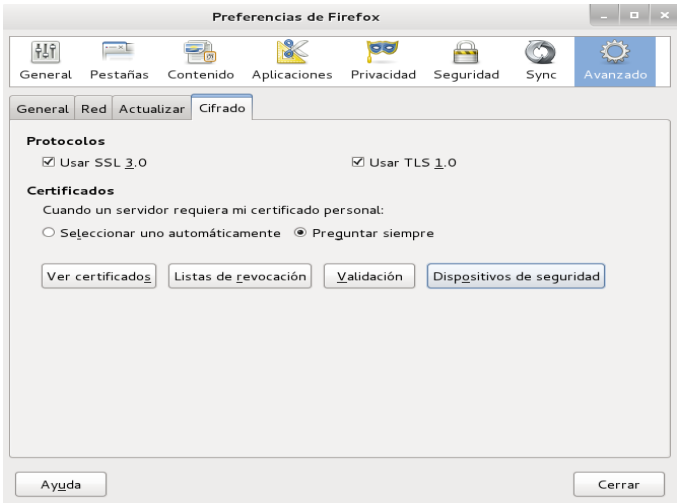
Navegadores web

Firefox

Firefox es uno de los navegadores mas usados en la actualidad.

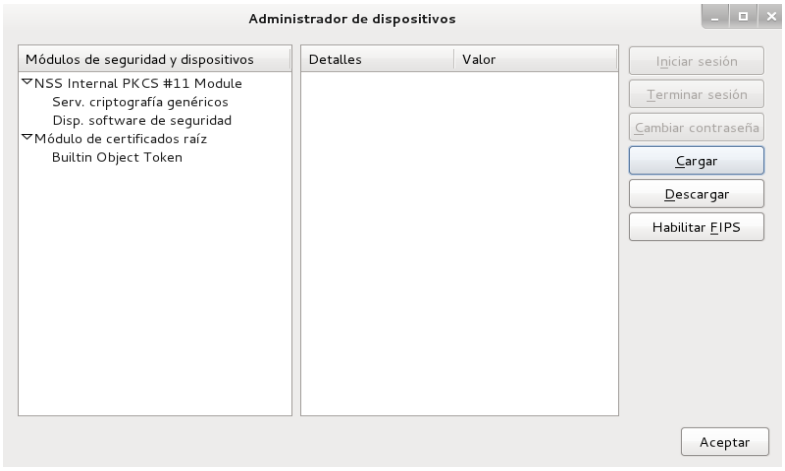
Instalación de módulo para certificados

En el menú Firefox → *Opciones* hacemos “click” sobre *Avanzado* y a continuación sobre la pestaña de *Certificados*, 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 instalados 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*.

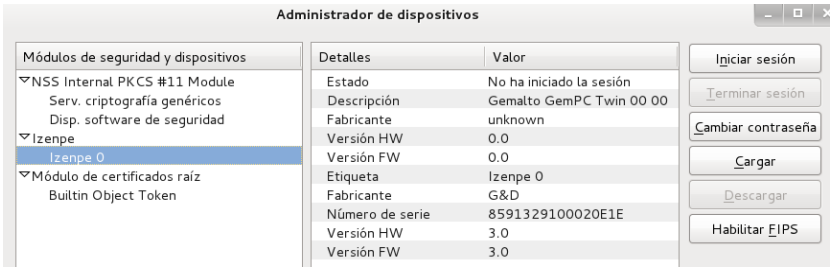


Se nos abre una ventana que nos permite definir un nuevo módulo PKCS#11 en el que:

- Nombre del módulo: un nombre genérico que haga referencia al módulo de seguridad para el Middleware. Introducimos un nombre cualquiera. Por ejemplo: Izenpe

- Archivo del módulo: le damos a Examinar y navegaremos hasta la ruta donde se encuentra el archivo `bit4ipki.dll` (`Equipo->C:/->windows->System32->bikt4ipki.dll`)

Después, hacemos “click” en aceptar y veremos como se nos añade el nuevo módulo.



Nota: *Si por un casual al añadir el módulo aparece vacío, puede ser que necesite reiniciar el equipo. Asegúrate de que tanto el lector como la tarjeta están correctamente conectados al PC*

Google Chrome

Actualmente, el navegador Google Chrome soporta la firma con certificados #PKCS11 sin necesidad de hacer ningún tipo de configuración extra.

Simplemente deberemos tener instalado el navegador antes de realizar la instalación tanto de Oracle Java, como de los certificados de Izenpe, en los cuales, durante la instalación, deberemos marcar la casilla de Google Chrome.

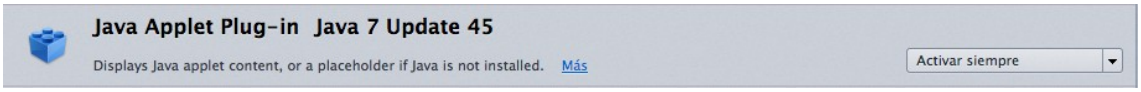
Ejemplo de uso de las aplicaciones

Identificación en sitios web

Firefox

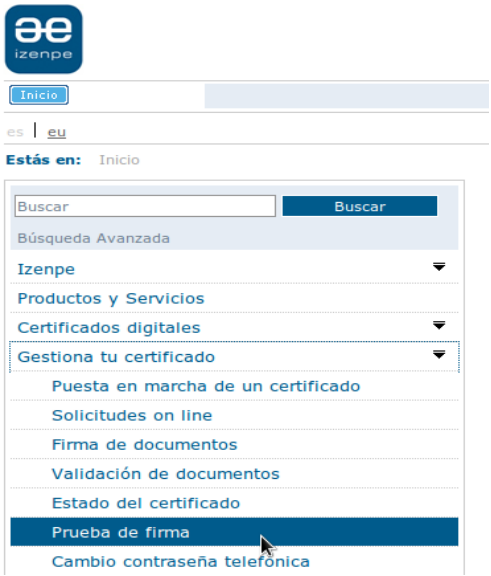
Una vez configurada la ubicación de los certificados según se ha explicado en el apartado correspondiente realizaremos una prueba de firma para comprobar que toda la instalación es correcta y el proceso se realiza satisfactoriamente.

Abrimos *Firefox → Complementos → Plugins* , revisamos si esta cargado el plugin de java y volvemos a comprobar la versión en la pagina web:



Verificar Versión de Java → http://www.java.com/es/download/installed.jsp

Cuando todo este correcto. Accedemos a la web de Izenpe (http://www.izenpe.com/), hacemos *"clic"* sobre ***Gestiona tu certificado*** y a continuación en **Prueba de Firma**.



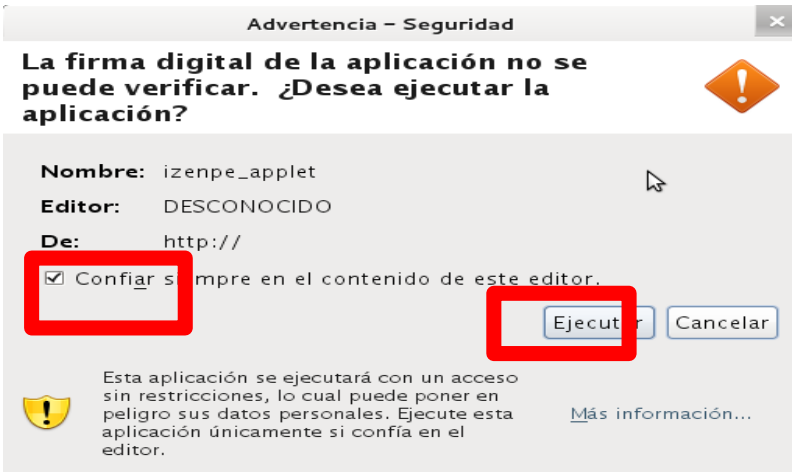
Permitiremos las Ventanas Emergentes

La primera vez que accedamos es posible que nos aparecerá una advertencia relacionada con permitir o no permitir las ventanas emergentes.

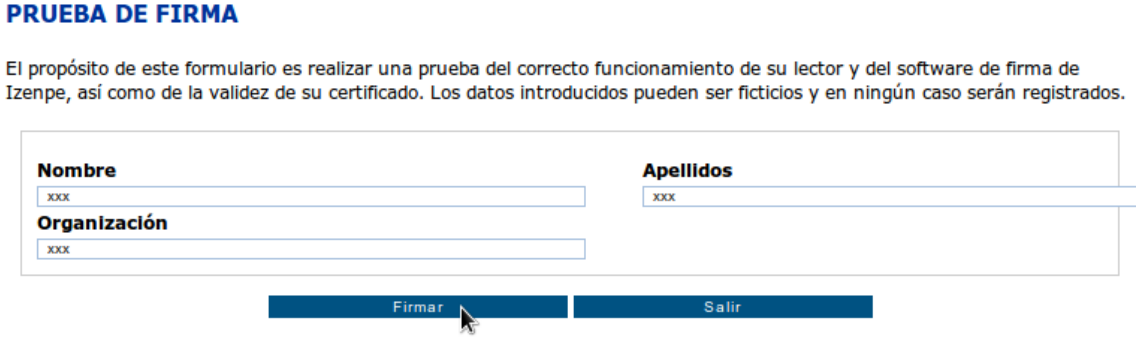
En este caso, permitiremos la ventanas emergente.

Si nos da la opción de permitir siempre para este sitio, la elegiremos.

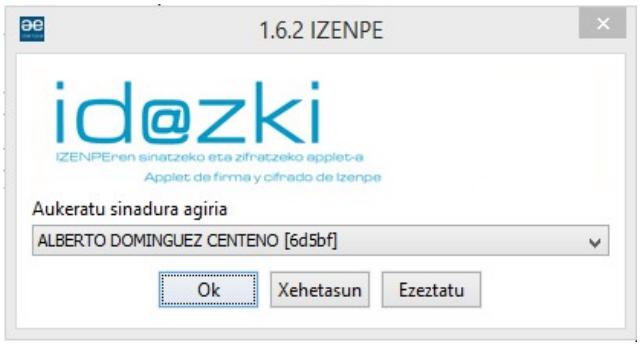
Nos saldrá una advertencia de seguridad en la cual es muy importante **ACTIVAR** la casilla de **CONFIAR SIEMPRE** y después darle a **EJECUTAR**.



Después se nos cargará una página en la que tendremos que poner unos datos para realizar la prueba de firma. No tienen por que ser reales, tal y como se muestra en la imagen.

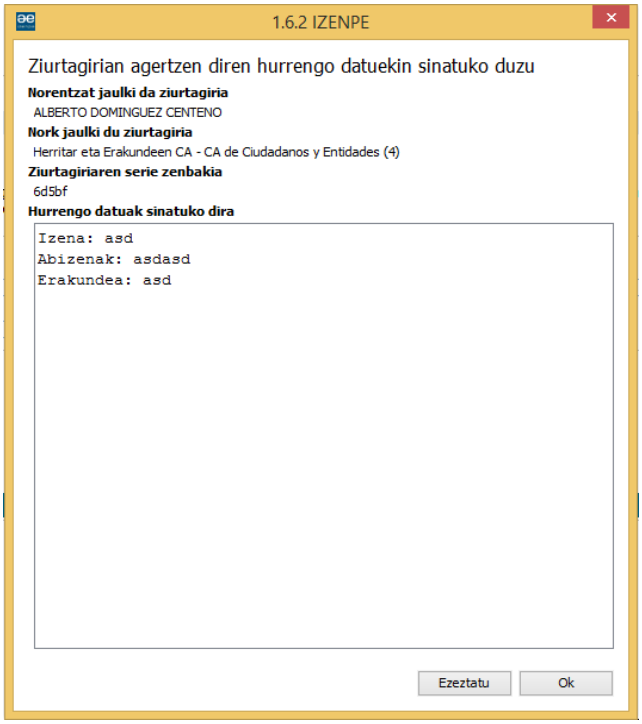


Le damos a firmar y elegiremos nuestro certificado con el que queremos firmar y le damos a aceptar.

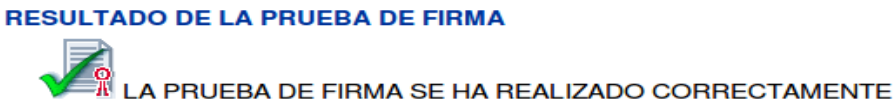


Posteriormente nos pedirá nuestro pin personal y lo introducimos.

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.



Se procesa la firma y cuando se complete nos aparecerá un mensaje confirmando que todo ha ido correctamente.



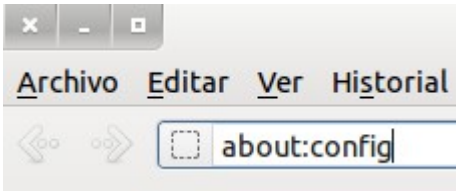
Nota: Es importante que cuando acabemos de realizar las gestiones oportunas cerremos la sesión del sitio web así como el navegador para evitar que otras personas puedan acceder a Internet con nuestros credenciales.

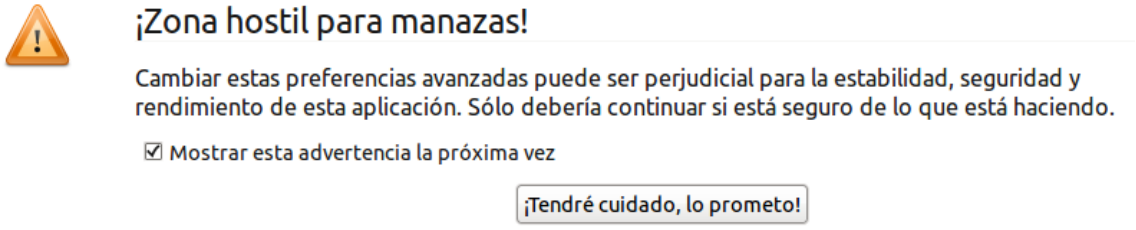
Cambio necesario en Firefox para que funcione el acceso en algunas Webs

Con el salto de las versiones de Firefox y los cambios realizados en cada versión del navegador, el acceso o la ejecución de ciertos servicios en algunas paginas webs se ha visto "capado" produciendo algunas incompatibilidades.

Por ejemplo, para acceder a **Bizkaia.net** necesitamos modificar un valor en la configuración de Firefox. Y lo hacemos de la siguiente manera:

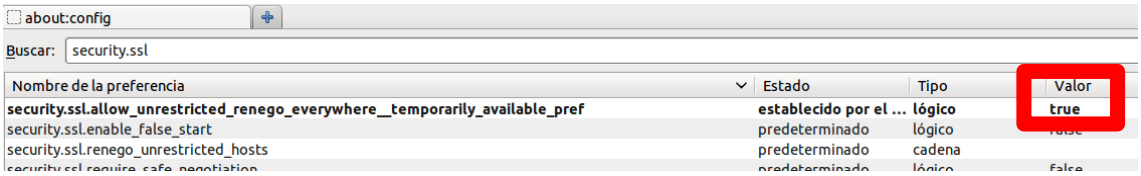
Abrimos Firefox y escribimos en el campo de url: *about:config*





Aceptamos haciendo click en ¡Tendré cuidado, lo prometo! y escribimos en el buscador: *security.ssl*

Hacemos doble click sobre la primera opción que nos encuentra, y veremos que, además de resaltar en negrita, cambia su valor a **TRUE**.



security.ssl.allow_unrestricted_renego_everywhere__temporarily_available_pref

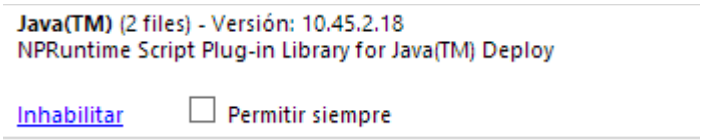
Cerramos la pestaña y ya podremos acceder correctamente con nuestra tarjeta en Bizkaia.net

Google Chrome

Una vez realizados todos los pasos para *Google Chrome* según se ha explicados en sus apartados correspondientes, realizaremos una prueba de firma para comprobar que toda la instalación es correcta y el proceso se realiza satisfactoriamente.

Comprobar Plugin de Java

Para comprobar si esta correctamente cargado y funcionando Java, abrimos una nueva pestaña en el navegador y escribimos como url: chrome://plugins



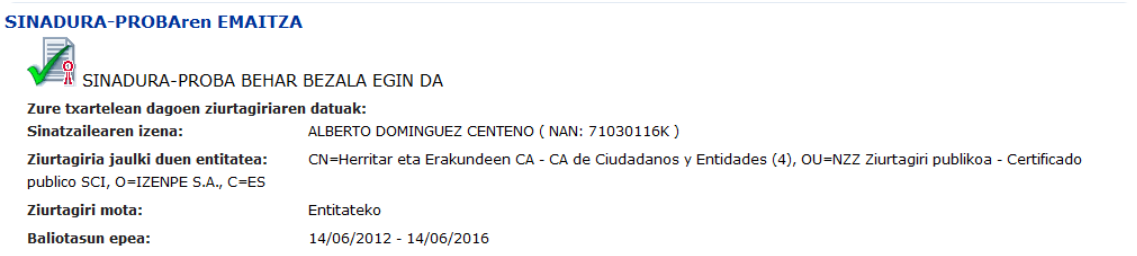
Podremos observar un listado de los plugins instalados, entre los que se ha de encontrar Java.

Una vez comprobado el Java, podemos realizar la prueba de firma en la web de Izenpe.

Prueba de Firma

El proceso es el mismo que el visto en el apartado anterior para el navegador Firefox.

El resultado final, de estar todo correcto, será el siguiente:



Firma de documentos ofimáticos

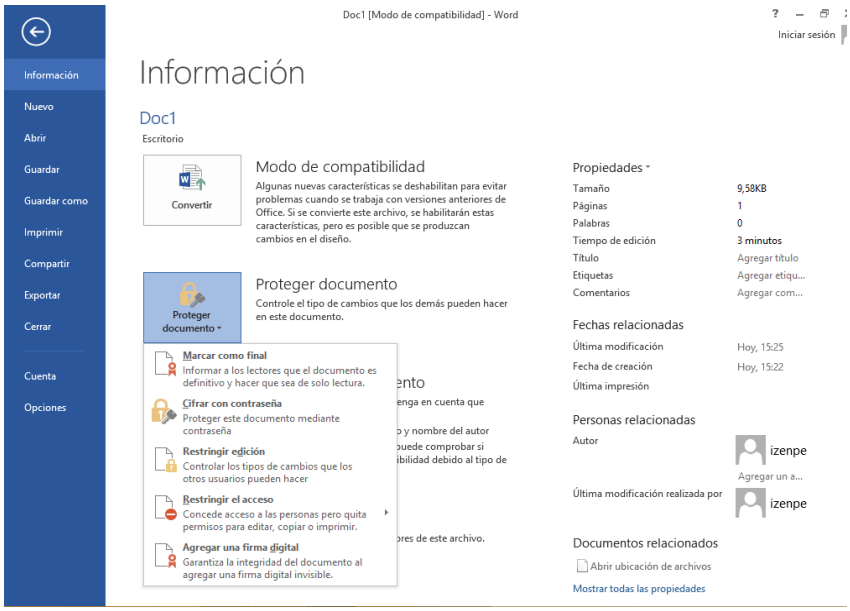
Microsoft Office

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.

LibreOffice permite firmar los siguientes tipos de documentos:

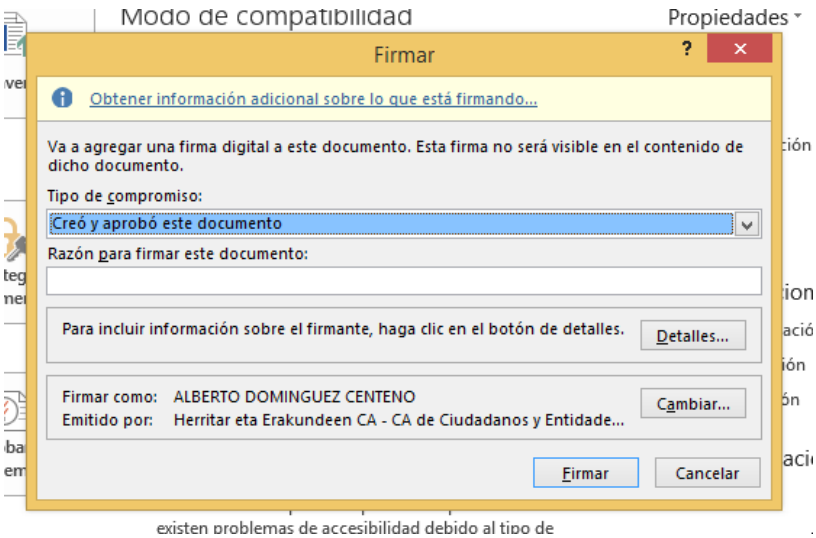
- Documentos de texto
- Hojas de cálculo
- Presentaciones
- Dibujos

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

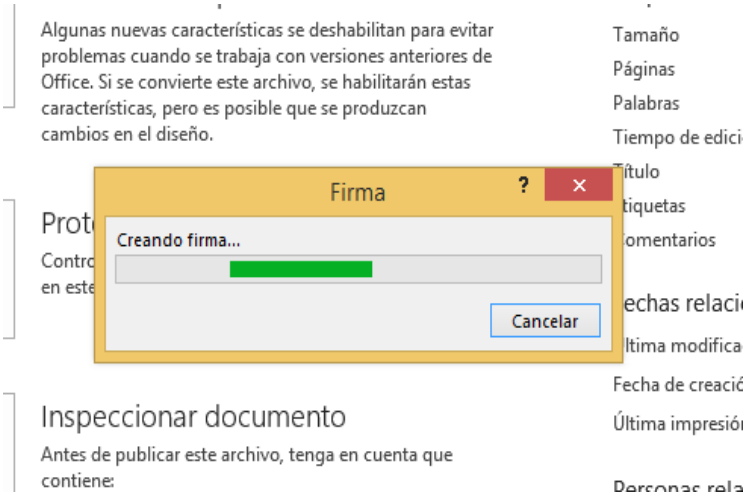


Nota: La firma del documento es necesario realizarla sobre un documento guardado, que no se va a modificar. En el momento en que se firma el documento si se modifica se pierde la firma y es necesario volver a firmarlo.

Una vez guardado nos muestra el gestor de firmas digitales de Microsoft Office



Elegimos la opción de tipo de compromiso que nos parezca adecuado y le damos a firmar.

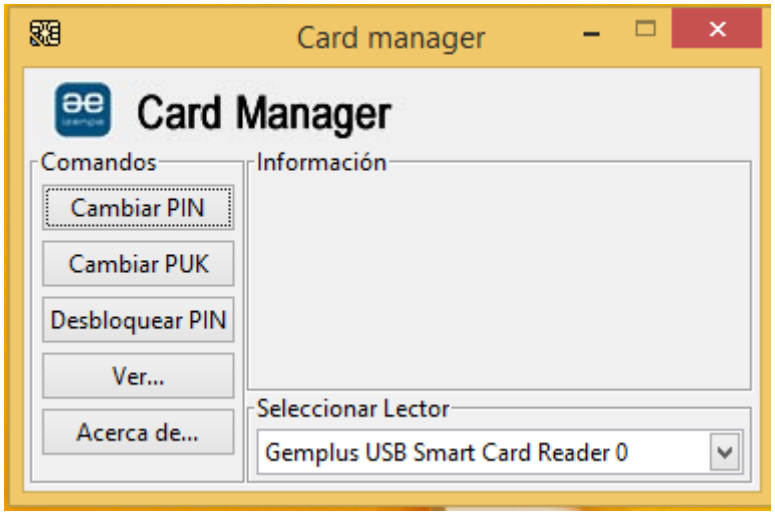


Otras aplicaciones adicionales

Gestor de la Tarjeta de Izenpe

Junto con el Middleware descargado, viene una aplicación con la cual podremos cambiar el PIN, desbloquearla introduciendo el PUK (por si hemos introducido tres veces el PIN mal y se ha bloqueado), y alguna que otra opción.

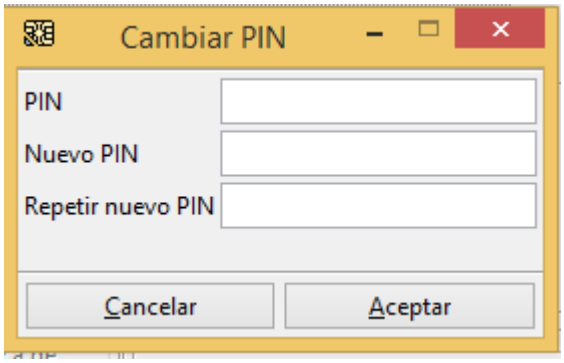
Podremos encontrarla junto a las demás aplicaciones, además se nos creara un acceso directo en el escritorio.



Cambio de PIN

Le daremos a la opción cambio de PIN dentro de la aplicación Card Manager

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

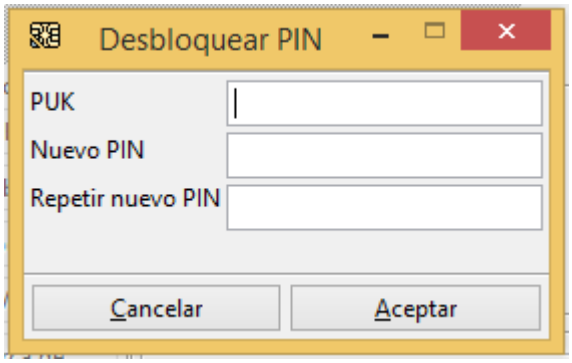


Nota: *Recomendamos el uso de la propia aplicación de Izenpe para hacer este tipo de modificaciones.*

Desbloqueo de PIN

Cuando realizamos operaciones con nuestra tarjeta criptográfica es posible que de vez en cuando introduzcamos erróneamente el PIN, estos dispositivos son sensibles a este tipo de errores y pueden causar bloqueos.

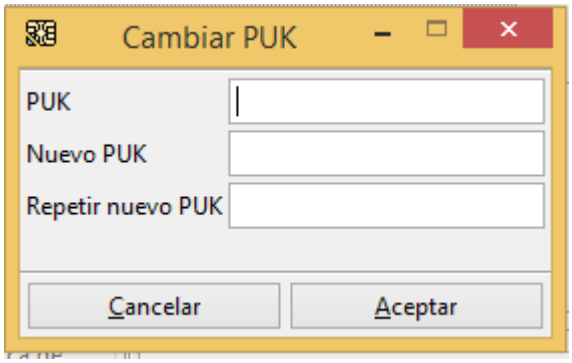
Para solucionar estos problemas existe una opción de desbloqueo de PIN.



Cambio de PUK

El PUK es un numero de seguridad que necesitaremos para hacer cualquier tipo de modificación sobre la tarjeta.

Para proceder a hacer un cambio del mismo procederemos de igual manera que lo haríamos para cambiar el PIN.



Ver...

Esta opción nos mostrara información sobre el certificado correspondiente a la tarjeta, también nos servirá para comprobar que el ordenador esta reconociendo bien tanto la tarjeta, como el lector de tarjetas.

Incompatibilidades conocidas (Importante)

DNIe

Es conocido que existen conflictos cuando disponemos de la instalación necesaria para funcionar con el DNIe y la necesaria para las tarjetas Izenpe.

En las ultimas versiones deberían de poder convivir ambas.

Nota Importante: Izenpe no se hace responsable del soporte o problemas relacionados con el DNIe.

Tarjetas Antiguas de Izenpe

Con el cambio de fabricante en las tarjetas de Izenpe, se producen dos casos a destacar:

· Las tarjetas antiguas (anteriores al 2012), funcionan con el nuevo Middleware y la nueva instalación.

· Las tarjetas nuevas, no funcionan en instalaciones antiguas (realizadas con las librerías OpenSC). Necesitan el nuevo Middleware para que funcionen correctamente.

Anexo para Sistemas Móviles

Windows Phone

A día de hoy en las versiones de Windows Phone 7 en adelante no es necesario la instalación de certificados raíz para poder navegar sin avisos de error por paginas que los soliciten, están ya incluidos en el navegador del sistema.

Acerca de

Este documento ha sido elaborado por la empresa Irontec Internet y Sistemas sobre GNU/Linux.

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.