GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES
SECRETARÍA DE ESTADO PARA LAS ADMINISTRACIONES TERRITORIALES

Aura
Subvenciones para catástrofes naturales

APLICACIÓN AURA

PLATAFORMA DE SUBVENCIONES PARA CATÁSTROFES NATURALES

MANUAL DE FIRMA

Entidades Locales Solicitantes

Índice

1 Requisitos generales

1.1 Requisitos técnicos

El servicio de firma electrónica proporcionado por el MINHAFP, admite todos aquellos certificados de persona física reconocidos por la plataforma @firma.

De forma general las configuraciones soportadas son:

- Windows XP, Windows Vista, Windows 7 y Windows 8. La arquitectura soportada de todos los sistemas operativos es 32 y 64 bits. En todos los casos, la máquina virtual Java (JVM) instalada tiene que ser de 32 bits.
- Navegadores: Internet Explorer o Mozilla Firefox. **Para el proceso de la firma sólo se podrá usar el navegador Internet Explorer**.
- Es necesario tener instalada la versión de la máquina virtual Java 8 Update 45 (1.8u45) de 32 bits. La última máquina virtual Java distribuida por Oracle se puede descargar o actualizar en el enlace: https://www.java.com/es/download/.

1.2 Requisitos previos

De cara a la utilización de los certificados, además de cumplir con los requisitos técnicos, es importante verificar que:

- El certificado esté correctamente instalado en el navegador que se va a utilizar para la realización de la firma de acuerdo a las instrucciones facilitadas por el emisor del mismo.
- El certificado emitido no está caducado ni revocado.

2 Configuración

2.1 Si utiliza Internet Explorer

2.1.1. Incluir la web de la aplicación como sitio de confianza del navegador:

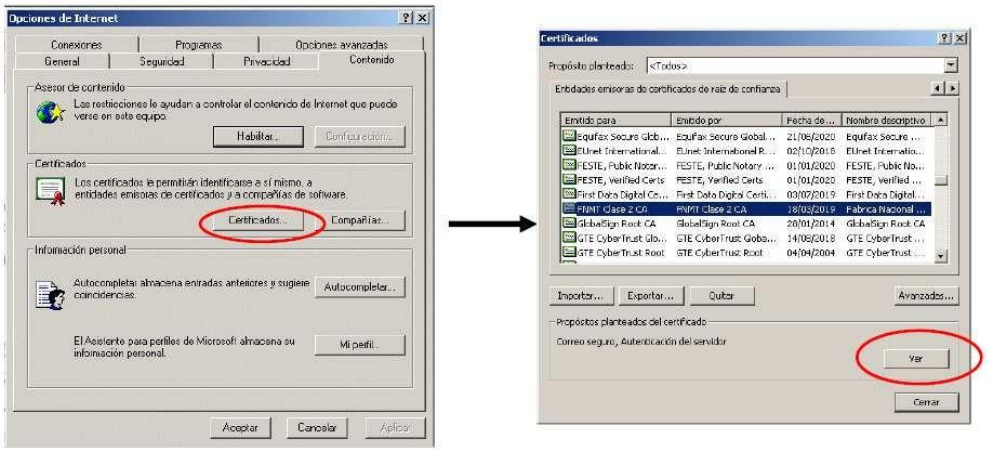
`Herramientas > Opciones de Internet > Seguridad > Sitios de confianza.`
A continuación pulsar el botón Sitios y agregar la dirección *https://aura.redsara.es/*

2.1.2. Configuración de las propiedades del certificado raíz de nuestro certificado de firma:

Los certificados de firma aceptados, pueden ser emitidos por cualquiera de las entidades listadas con anterioridad. Aquí pondremos como ejemplo la FNMT, el cual es el caso más habitual.

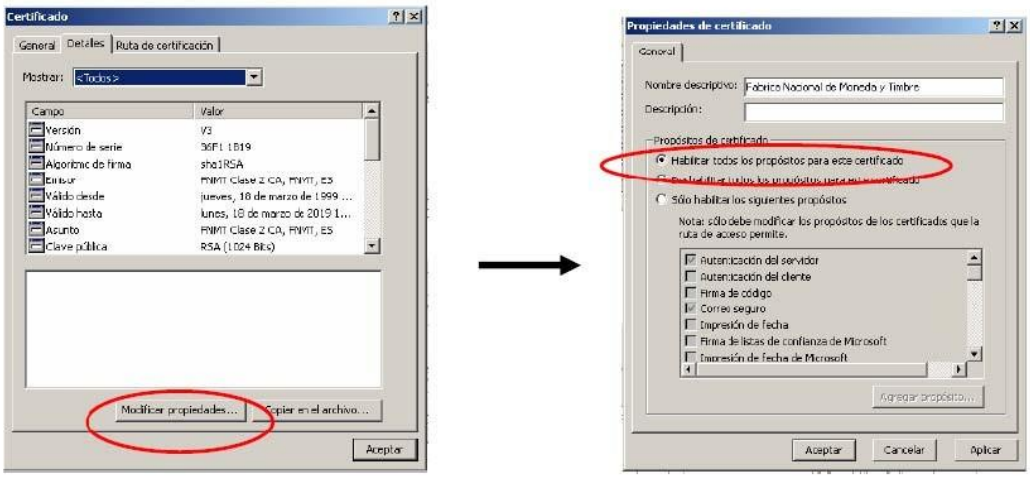
Para cambiar las propiedades de este certificado:

`Herramientas > Opciones de Internet > Contenido > Certificados > Entidades emisoras de certificados raíz de confianza.`
Marcar el certificado FNMT Clase 2 CA (o su correspondiente entidad emisora raíz) y pulsar el botón `Ver`:



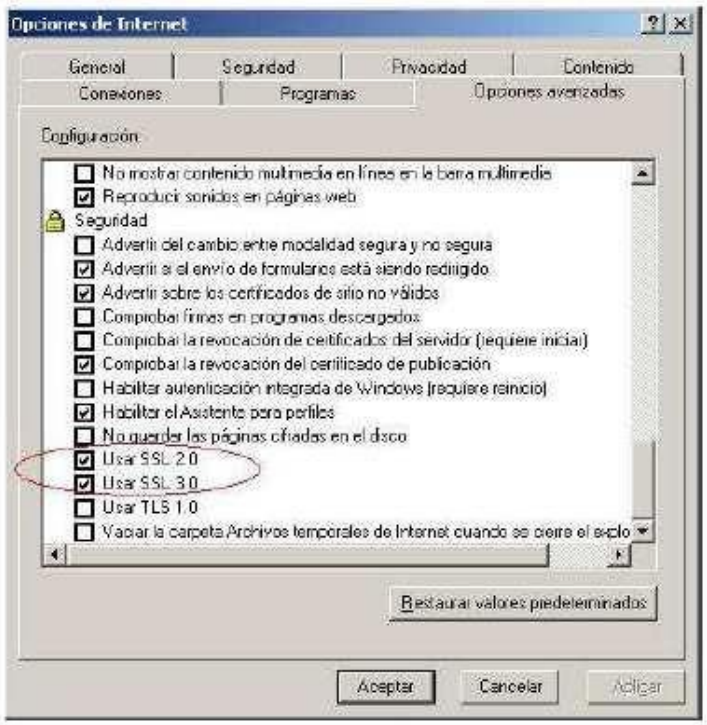
A continuación, pulsar la pestaña `Detalles` y al botón `Modificar propiedades...`.

Marcar la casilla `Habilitar todos los propósitos para este certificado` y pulsar el botón `Aceptar`.



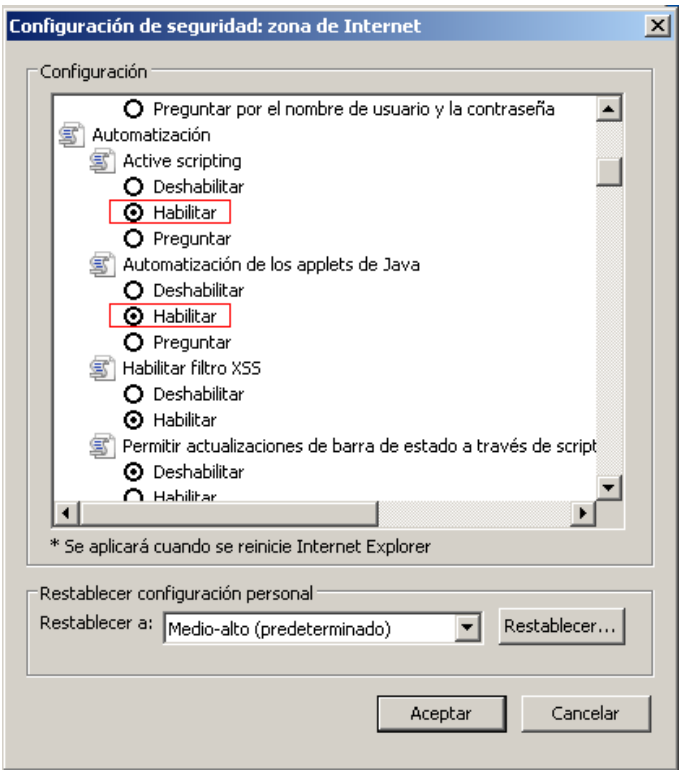
2.1.3. Activación de SSL3:

`Herramientas > Opciones de Internet > Opciones Avanzadas` y marcar las casillas correspondientes:



2.1.4. Activación Javascript

```
Herramientas > Opciones de Internet > Seguridad > Internet > Nivel
personalizado > Automatización:
  > Active scripting.
  > Automatización applets de Java.
```



2.1.5. No guardar páginas cifradas en el disco:

`Herramientas > Opciones de Internet > Opciones avanzadas >Seguridad:`

Desactivar el marcador de la opción `No guardar las páginas cifradas en el disco:`