GOBIERNO DE ESPAÑA

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL

Manual de usuario – Configuración de Java para la firma electrónica mediante *applets*

Aplicaciones con sistema de firma no normalizado tipo 1 (solución *Applets*)

Dirección de Seguridad, Innovación y Proyectos

30/10/2017

Versión: 1.1

Clasificación: Público

Gerencia de Informática de la Seguridad Social

CONTROL DE VERSIONES			
Título		Documento tratamiento de firma Electrónica	
Autor		AISS	
Fecha versión 1.0		22/08/2017	
Versión	Fecha	Responsable	Cambios introducidos
1.1	30/10/2017	Dirección de Seguridad, Innovación y Proyectos	Primer Documento

INDICE

1. INTRODUCCIÓN

A medida que los sistemas operativos y navegadores de internet mejoran sus medidas de seguridad, los desarrollos han de adaptarse a las nuevas restricciones que los estándares van dictando. Una de estas restricciones afecta a los desarrollos web basados en Java, al que se le van descubriendo con cierta frecuencia vulnerabilidades que afectan al tratamiento de los datos y a la protección de los mismos.

Los procedimientos de firma electrónica, cada vez más frecuentes en el tratamiento e intercambio electrónico de información, requieren igualmente una vigilancia especial para no incurrir en vulnerabilidades o defectos de forma.

La Seguridad Social está comprometida en un proceso de modernización y mejora de seguridad en el desarrollo de sus aplicaciones. Esto implica que en sus servicios web actualmente conviven varios sistemas de firma, uno para aplicaciones normalizadas (basadas en el sistema de firma *JNLP*) y otro para aplicaciones que no están normalizadas. Éstas últimas, podrán optar por utilizar uno de los dos sistemas de firma no normalizados: **tipo 1 y tipo 2**.

El sistema de firma no normalizado tipo 1, seguirá las premisas correspondientes al sistema de firma mediante ***applets***, con los condicionantes de configuración propios de este sistema de firma que ya se conoce y que aún se sigue utilizando en muchos de los servicios web de la Seguridad Social, hasta que las aplicaciones se adapten por completo a sistemas normalizados, momento en el que desaparecerán.

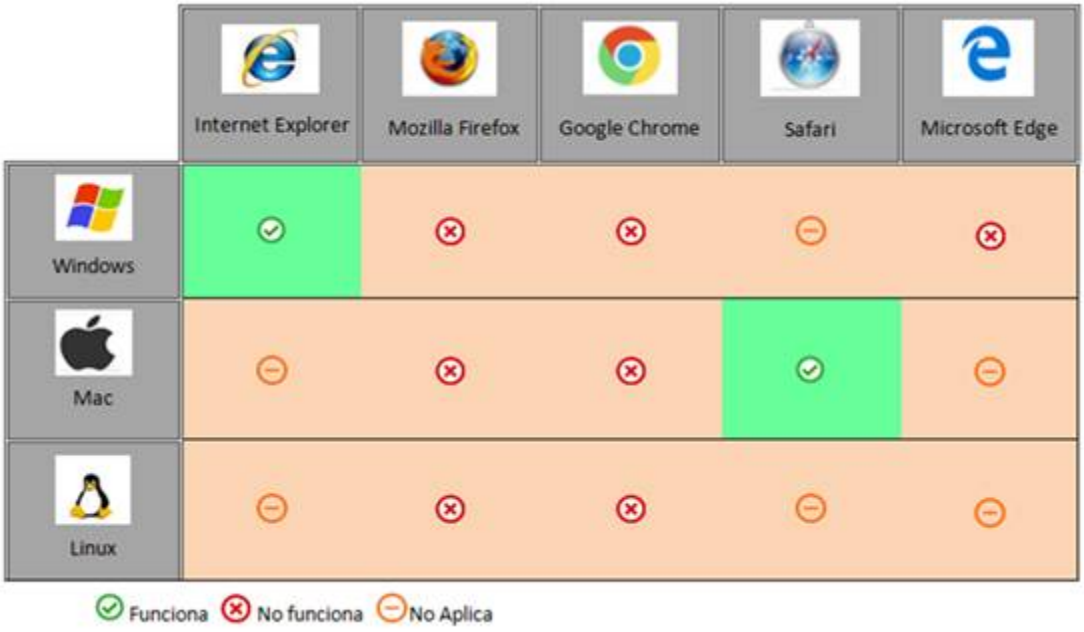
El sistema de firma no normalizado tipo 2, es un nuevo sistema de *firma en cliente* denominado ***CryptoBrowser***. Este nuevo sistema de firma sólo requiere la instalación de una pequeña aplicación en el *PC* del usuario y una extensión en el navegador de internet. Por el momento esta extensión sólo se ha desarrollado para el navegador *Chrome* y en sistemas *Windows.*

En la Sede se publica un documento con el listado completo de los servicios y sus sistemas de firma.

2. OBJETIVO

El presente documento describe el proceso del **sistema de firma no normalizado tipo 1** (mediante *applets),* así como la configuración específica de la máquina virtual de java para un correcto funcionamiento.

3. CUADRO DE COMPATIBILIDAD DE SISTEMAS OPERATIVOS Y NAVEGADORES EN EL SISTEMA DE FIRMA NO NORMALIZADO TIPO 1



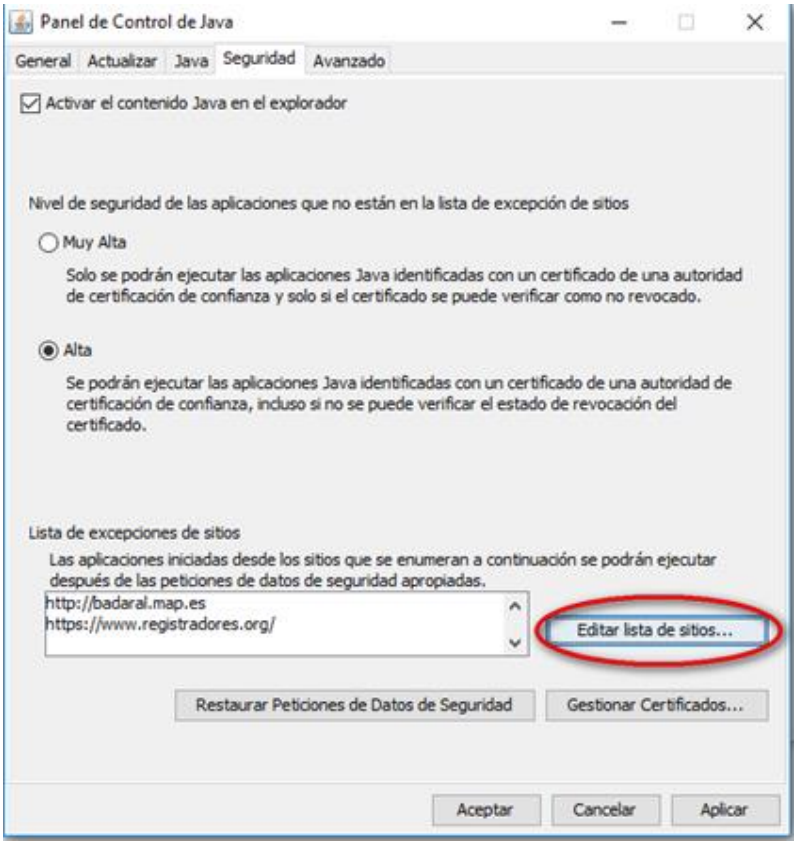
***NOTA.*- La configuración del navegador de internet compatible con este tipo de firma, podrá encontrarlo en el manual correspondiente**.

4. RECOMENDACIONES DE CONFIGURACION DE JAVA

4.1. Configuración de Java en procesos de firma mediante applets

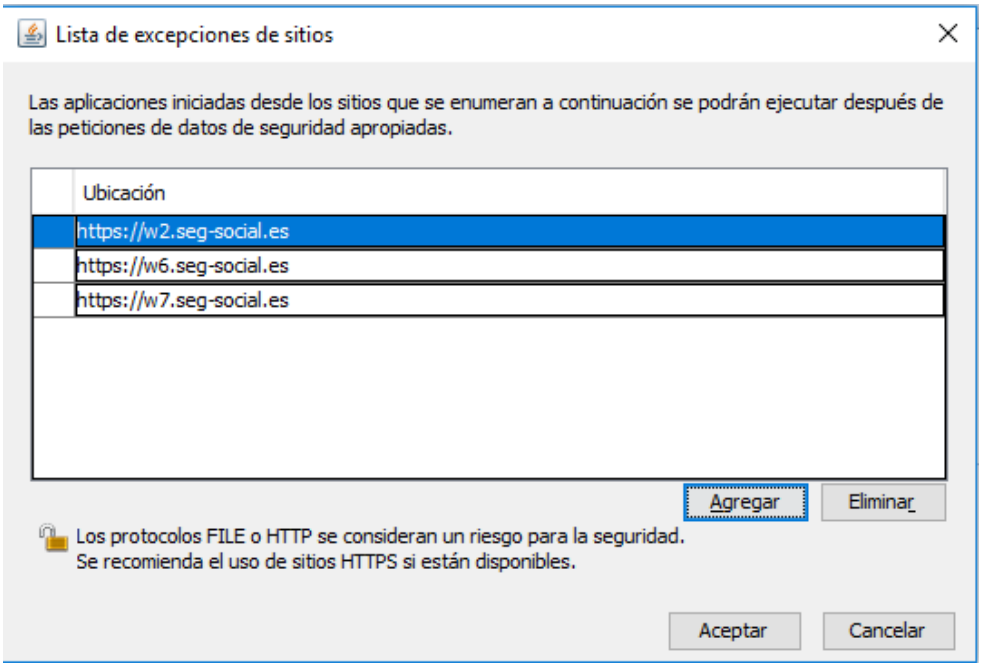
Acceda al panel de control de Java (*ver anexo: Acceder al panel de control de Java*)

Una vez en "Panel de control de Java" pulse en editar lista de sitios (Véase imagen)



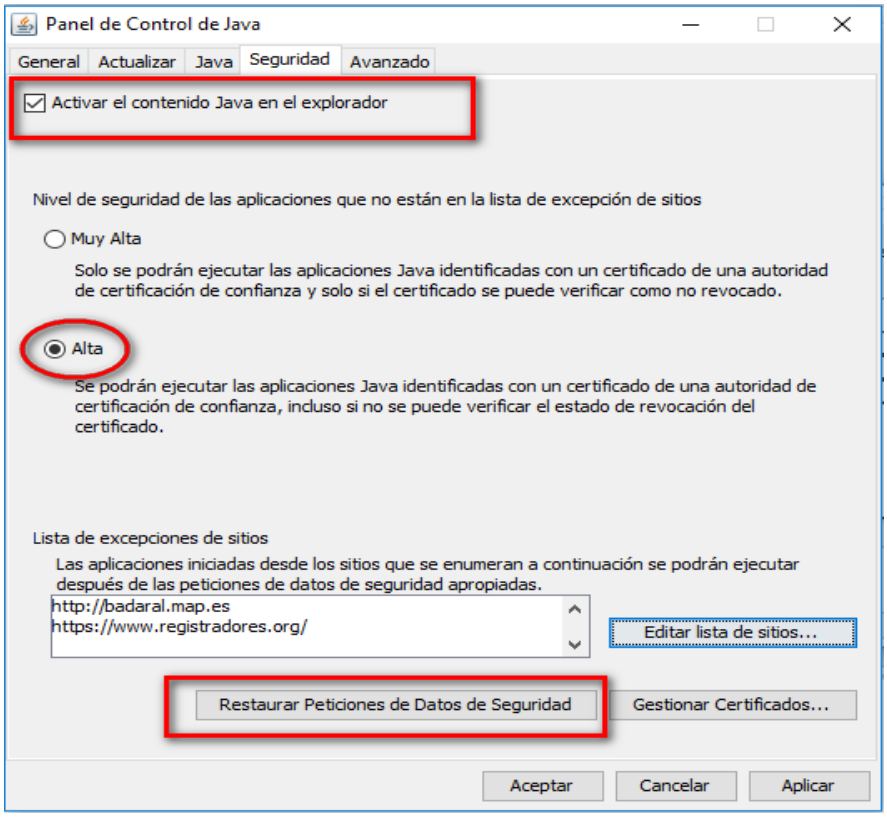
Pulse en agregar y añada las siguientes direcciones web:

- https://w2.seg-social.es
- https://w6.seg-social.es
- https://w7.seg-social.es



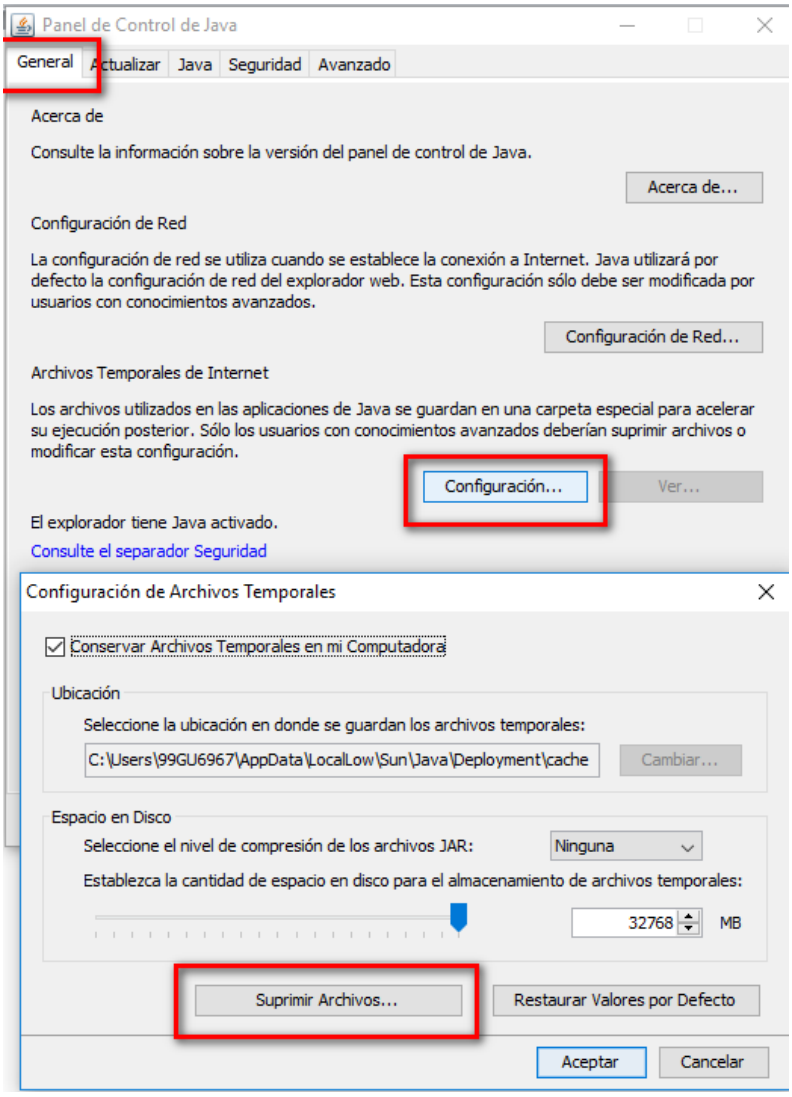
Pulse "*Aceptar*" y vuelva a la pestaña de seguridad. Marque las siguientes opciones:

- Activar el contenido java en el explorador
- Nivel de seguridad alta
- Restaurar peticiones de Datos de seguridad



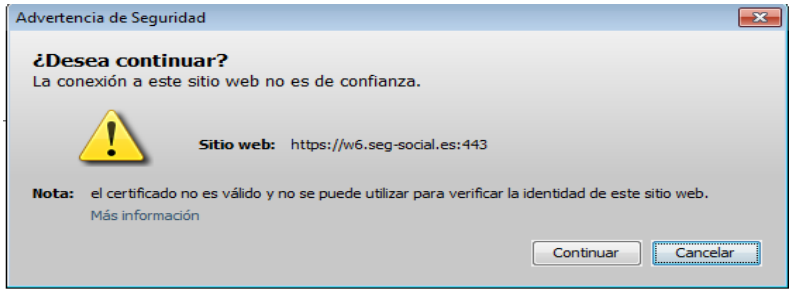
Acceda la pestaña General.

Botón: "*Configuración*" -> Botón: "suprimir archivos" -> Marcar las 3 opciones y aceptar.



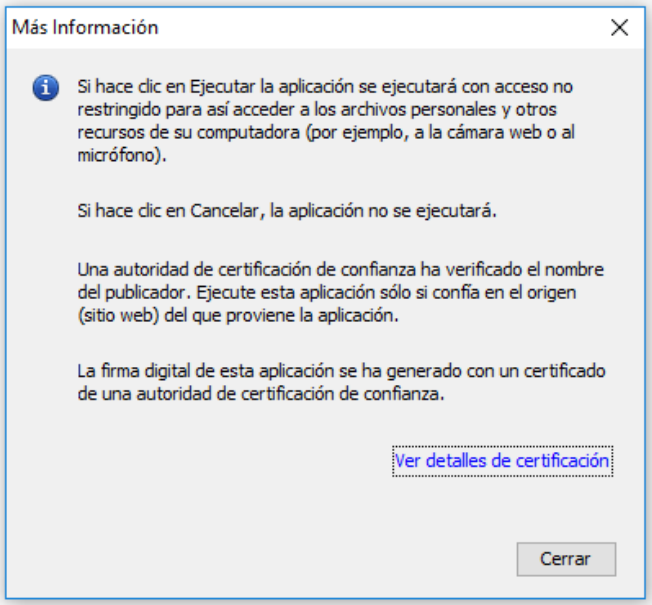
5. DESCRIPCIÓN DEL PROCESO DE FIRMA NO NORMALIZADO TIPO 1 (*APPLETS*)

Tras acceder al sitio web se nos pedirá verificar la autenticidad de la conexión, es decir, si confiamos en el servidor al que nos vamos a conectar. Para confirmar la confianza en el sitio pulsaremos sobre el botón continuar.

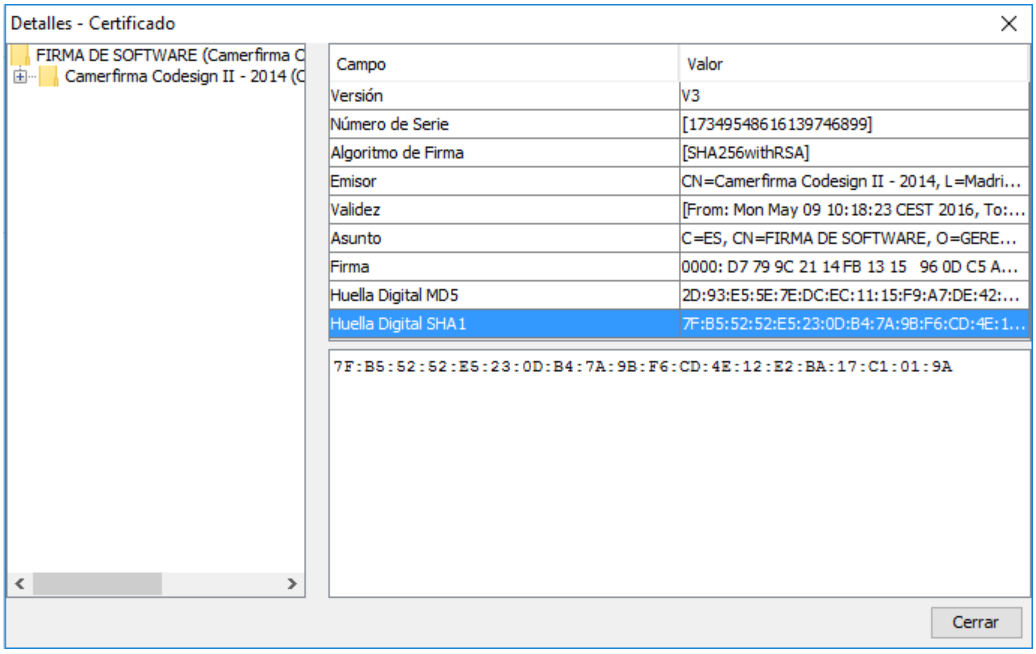


Tras acceder al sitio web se pedirá que confirmemos la confianza en el firmante del *applet*. Para saber si se confía en dicho firmante se puede mirar los datos del certificado que lo firma, para lo que accederemos a "Más información".

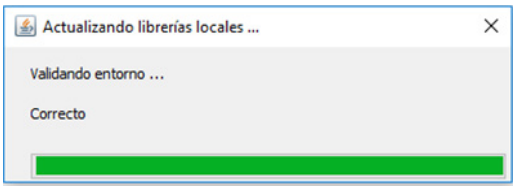
Aparecerá la siguiente ventana:



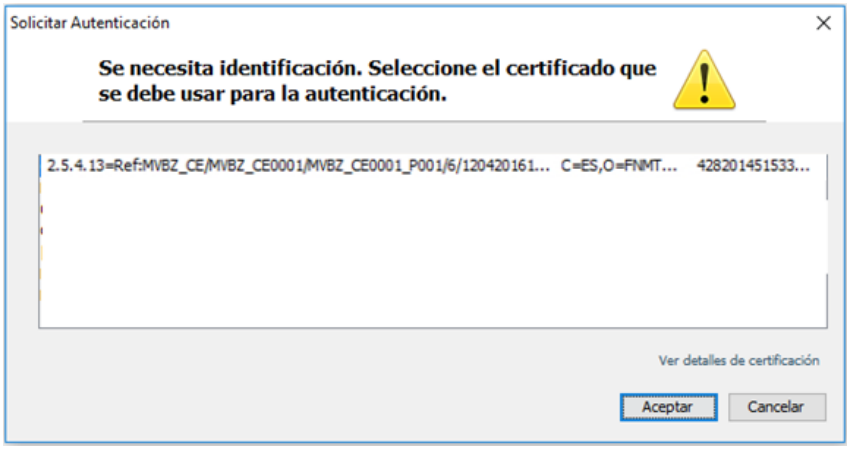
Al pulsar sobre "*Ver detalles de certificado*" le aparecerá la información concerniente al firmante del applet.



Una vez verificada la confianza en el editor pulsaremos sobre el botón “Ejecutar” para que se ejecute el *applet*.

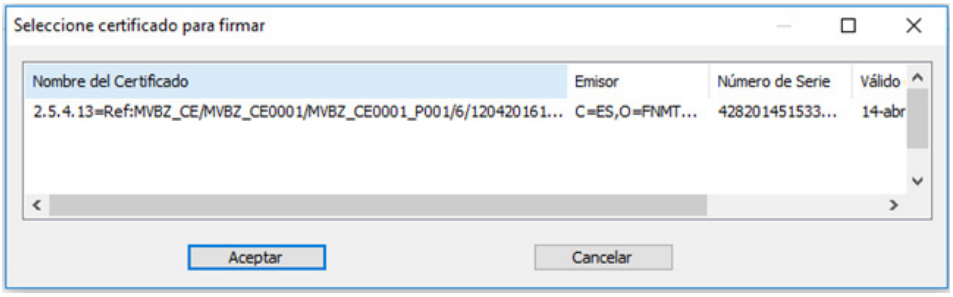


Es posible que nos solicite seleccionar el certificado.



Seleccione su certificado y pulse *Aceptar*.

Finalmente obtendrá la ventana de selección de certificado de firma. Aquí busque el certificado con el que desea realizar la firma, selecciónelo y pulse aceptar.



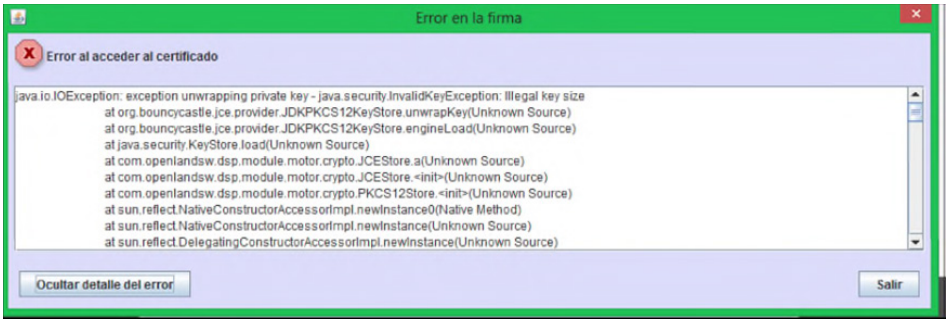
Una vez aceptado se iniciara el proceso de firma y ejecuta correctamente aparecerá una ventalla de confirmación de finalización de servicio.

6. POSIBLES INCIDENCIAS Y SOLUCIÓN

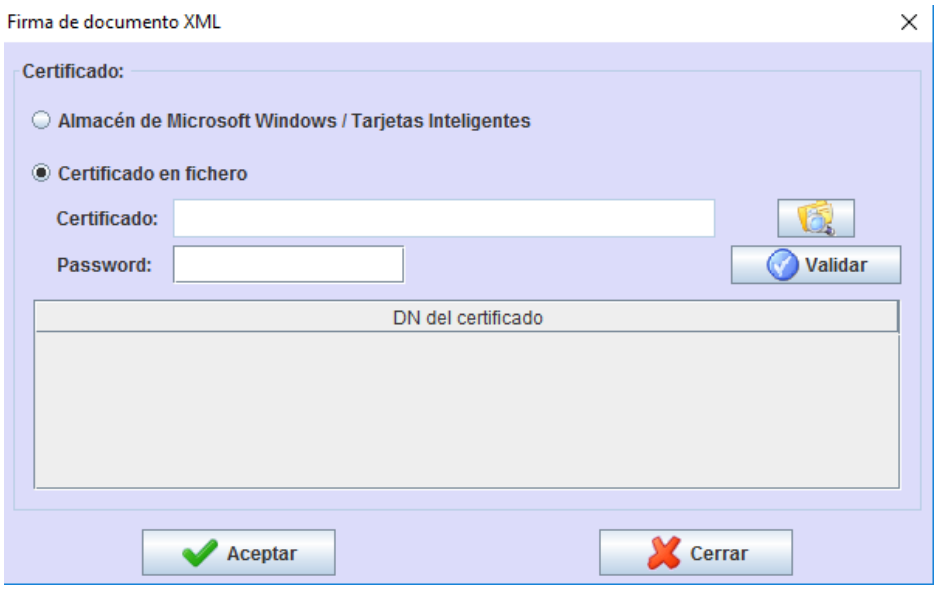
6.1. Error al acceder al certificado

6.1.1. Mensaje que se muestra

Error: Error al acceder al certificado



6.1.2. Explicación del error



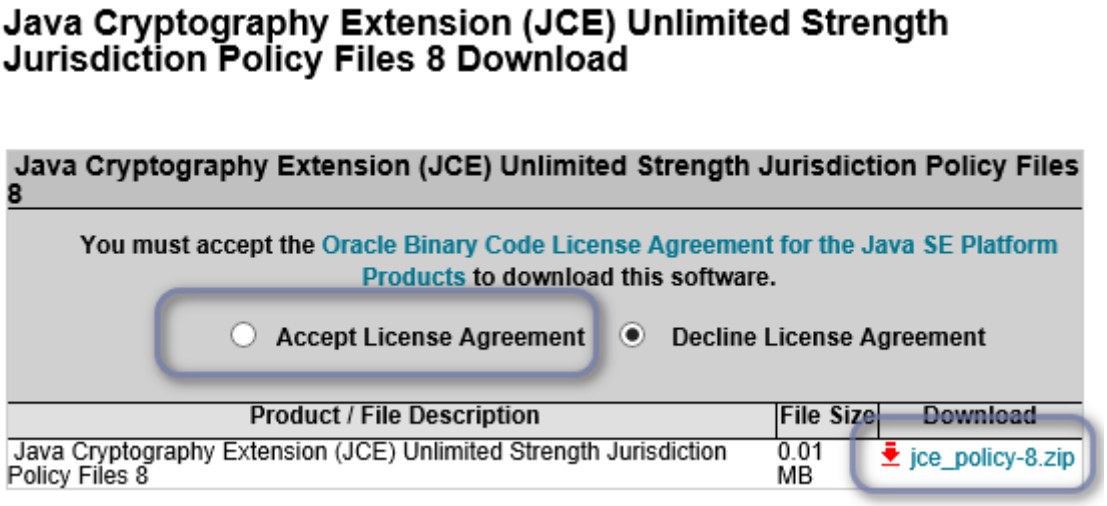
Solo si se escoge la opción de firma "Certificado en fichero" puede aparecer el error anterior.

Esto ocurre porque la longitud de clave no le permite realizar ese trámite.

6.1.3. Solución

Para solucionar y exceder el rango debe descargarse Java Cryptography Extension (JCE). Para ello, debe dirigirse a

http://run.gob.es/rxylje



Acepte el acuerdo de licencia y descargue el fichero jce_policy-8.zip. Se trata de un archivo comprimido que contiene a su vez tres rchivos.

Deberá descomprimir el archivo README.txt y ejecútalo con otro programa que no sea Bloc de Notas, por ejemplo WordPad o Notepad++.

En las instrucciones encontrara la ubicación donde tiene que descomprimir los otros dos archivos.

Ejemplo: C:\Program Files (x86)\Java\jre1.8.0_151\lib\security

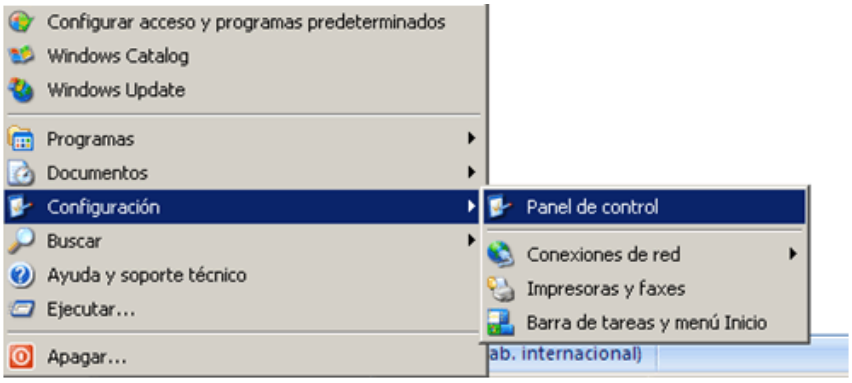
7. ANEXOS

7.1. Pasos para acceder a panel de control de Java

- **Paso 1**: Acceder al "Panel de Control de Windows".

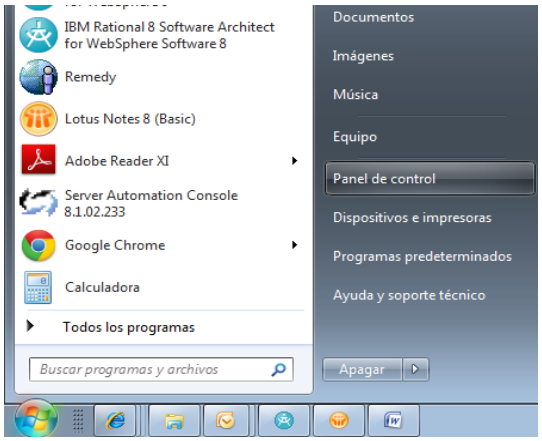
➢ *En Windows XP*

Seguir la ruta "Botón de Inicio / Configuración / Panel de Control".



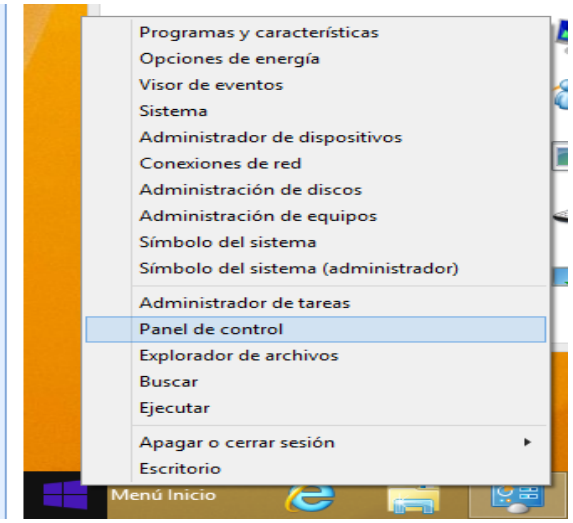
➢ *Windows Vista/7*

Seguir la ruta: "Botón Inicio / Panel de Control"



➢ *Windows 8 /10*

Seguir la ruta: Botón **derecho** sobre botón de Inicio (en la parte izquierda inferior de su pantalla). En el desplegable seleccione panel de control.



- ***Paso 2**: Acceder al panel de control de Java*

Según el tipo de vista mostrado en pantalla, las aplicaciones se dispondrán en forma de lista de iconos o por categorías. En el primer caso podrá distinguir el correspondiente a Java:

Si la vista está dispuesta por categorías, localice la aplicación del panel de control de Java dentro del grupo de aplicaciones "*Programas*"

8. COMUNICACIÓN DE INCIDENCIAS Y SUGERENCIAS

Si tiene problemas relacionados con el acceso a las aplicaciones, errores en el procesamiento de los datos, incidencias en el proceso de firma, tiene a su disposición el formulario del **Buzón de Consultas** en la página de la Seguridad Social:

http://run.gob.es/xmioxu