Preguntas frecuentes

Registro electrónico

Notificaciones electrónicas

Versión 2.0

certificado por DQS de acuerdo con
ISO 9001:2008
N° de reg. 229846 QM08

ÍNDICE

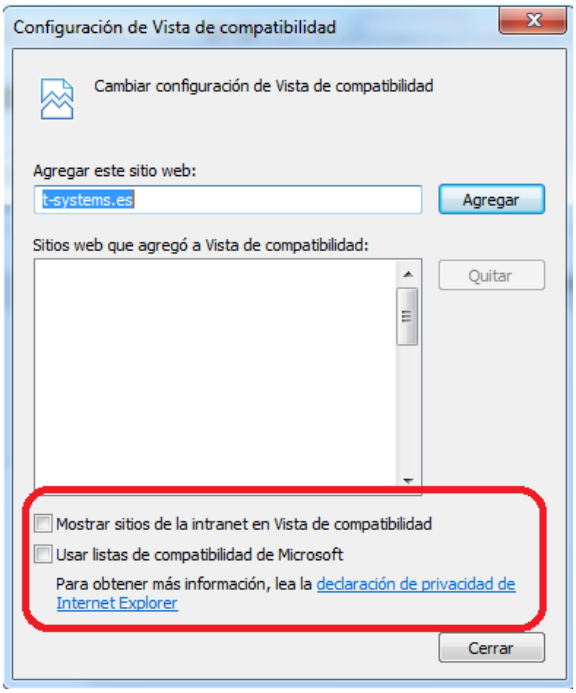
1 Windows – Internet Explorer

1.1 Versiones navegador

Las versiones de Internet Explorer soportadas son IE 9 o superior.

1.2 Vista compatibilidad

Hay que tener desactivada la vista compatibilidad en Internet Explorer tal y como se aprecia en la imagen.

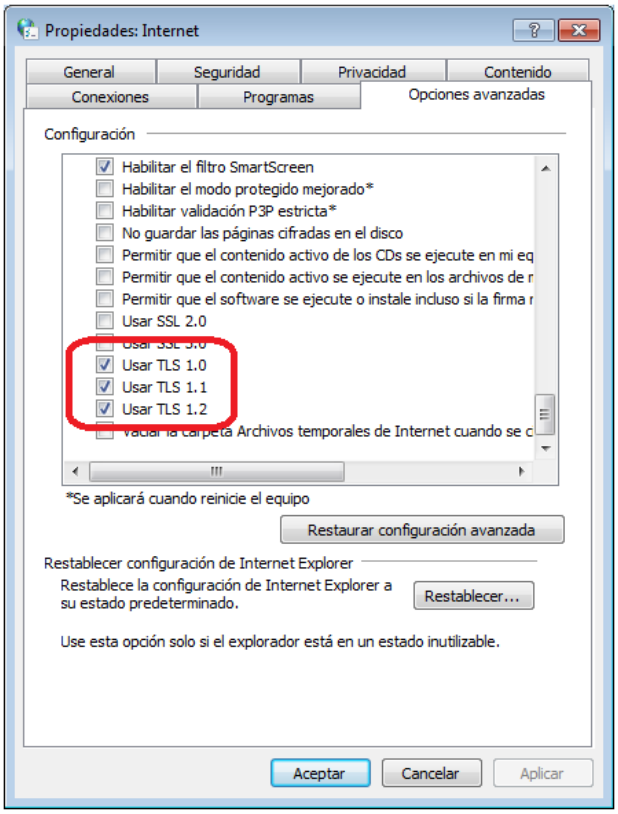


1.3 JNLPS

Si se produce un error al acceder al detalle de una solicitud de STA indicando que no hay aplicaciones instaladas para abrir este tipo de vínculos (JNLPS), el problema se debe a la instalación de Java. En esos casos significa que, o bien no está instalada la versión correcta de Java (mínimo la 1.8_74 o superior), o bien hay que reinstalar Java porque hay algún tipo de problema con la versión instalada.

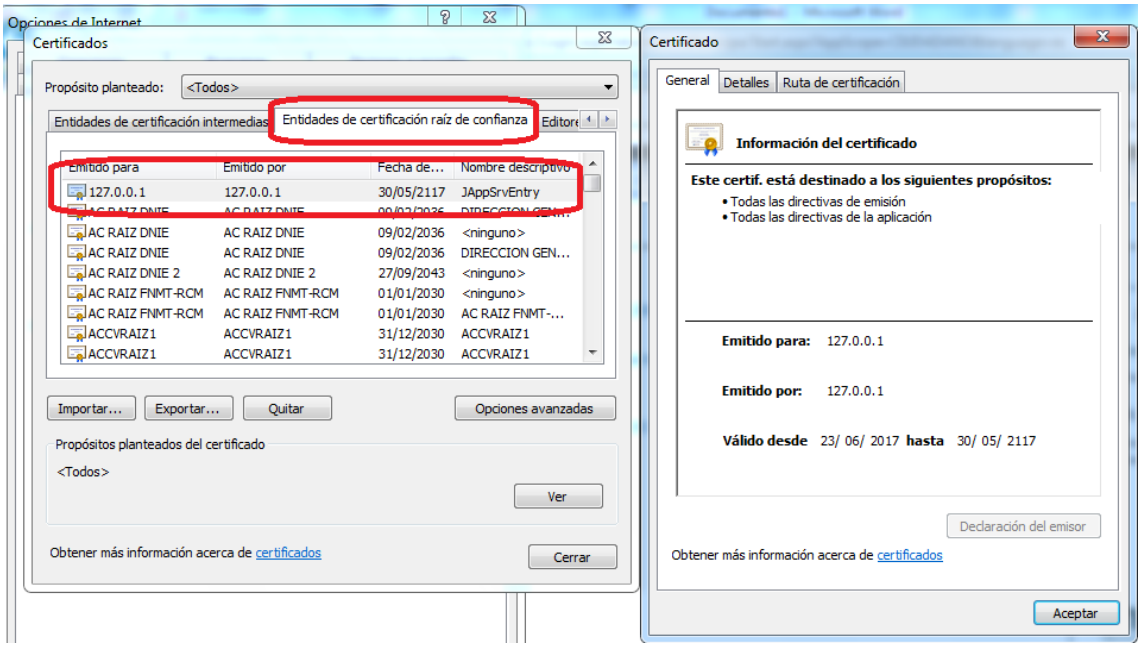
1.4 Protocolos TLS

Revisar que los protocolos TLS 1.1 y TLS 1.2 están activos en el navegador. Para activarlo hay que ir a "Opciones de Internet >> Opciones Avanzadas >> Seguridad" (es posible tener activado el SSL 3.0 y TLS 1.0). Las opciones deben estar como pueden verse en la imagen siguiente. Si las opciones que están marcadas en la imagen no lo estuvieran, es posible que Internet Explorer no pueda completar la conexión SSL contra el Registro Electrónico.



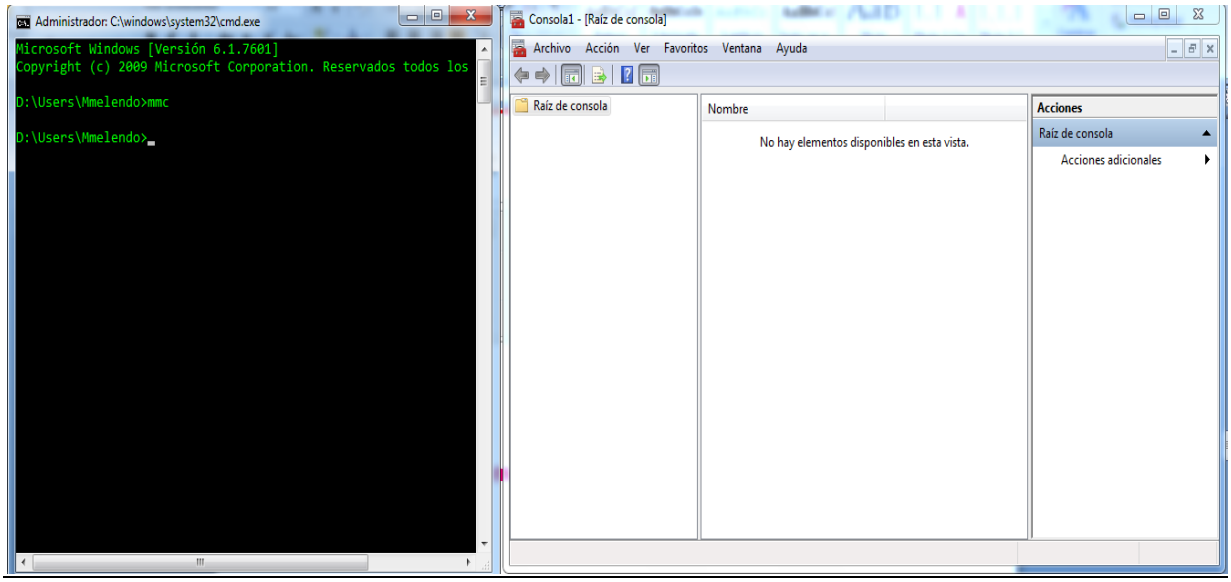
1.5 Instalación del certificado del applet de firma

Para el correcto funcionamiento del Registro Electrónico y las Notificaciones Electrónicas, habría que comprobar si el certificado del applet de firma se ha instalado correctamente en el navegador. Para ello tendríamos que dirigirnos a las opciones de Internet Explorer, "/Opciones de internet/Certificados" y seleccionar la pestaña "Entidades de certificación raíz de confianza". Allí debe de estar el certificado del applet, tal y como puede verse en la imagen de bajo. En el caso de que el certificado no se haya instalado o se haya instalado en otra pestaña distinta a la indicada, tendremos que realizar la instalación del certificado manualmente. Para ello deberemos seguir los pasos que se describen a continuación.

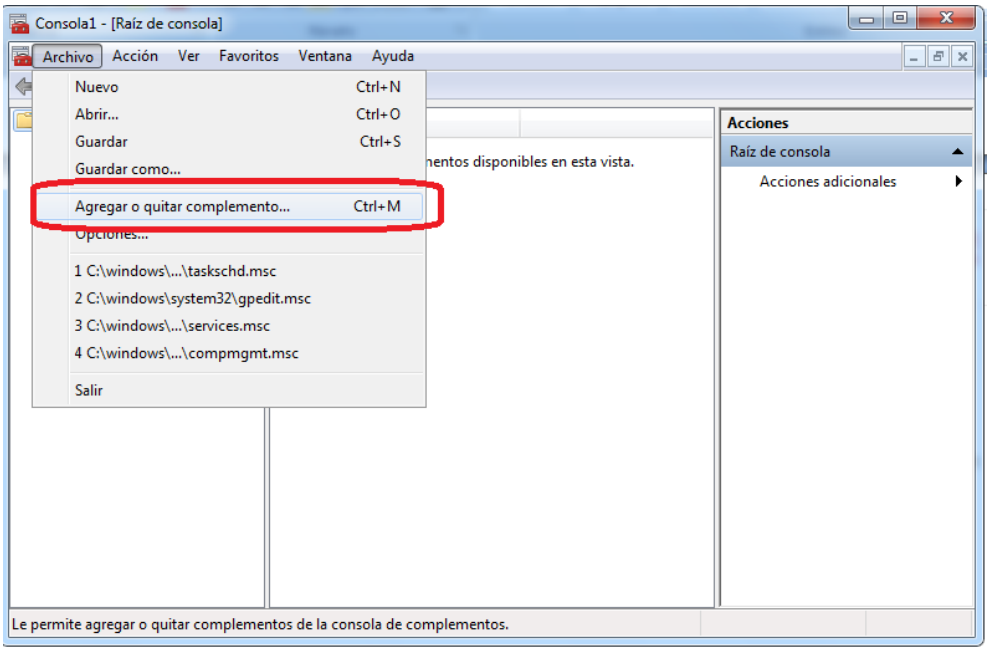


1.5.1 Instalación manual del certificado del applet

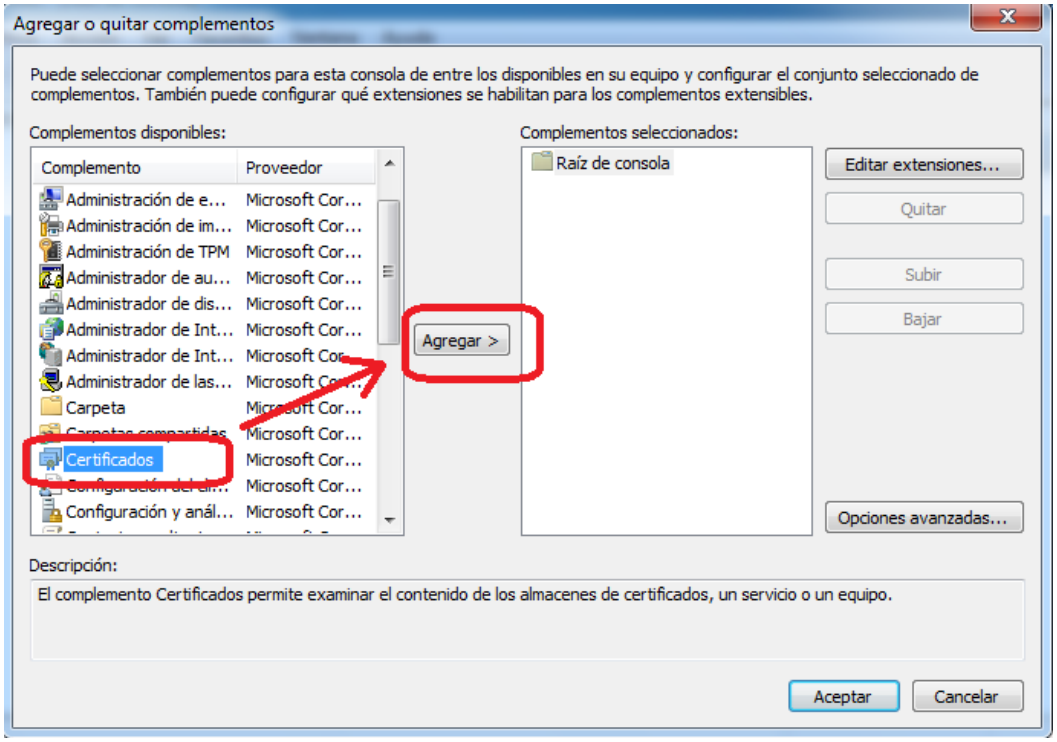
1.- Desde una consola de Windows ejecutaremos el comando “mmc” (sin las comillas) que nos abrirá una pantalla como la que puede verse bajo.



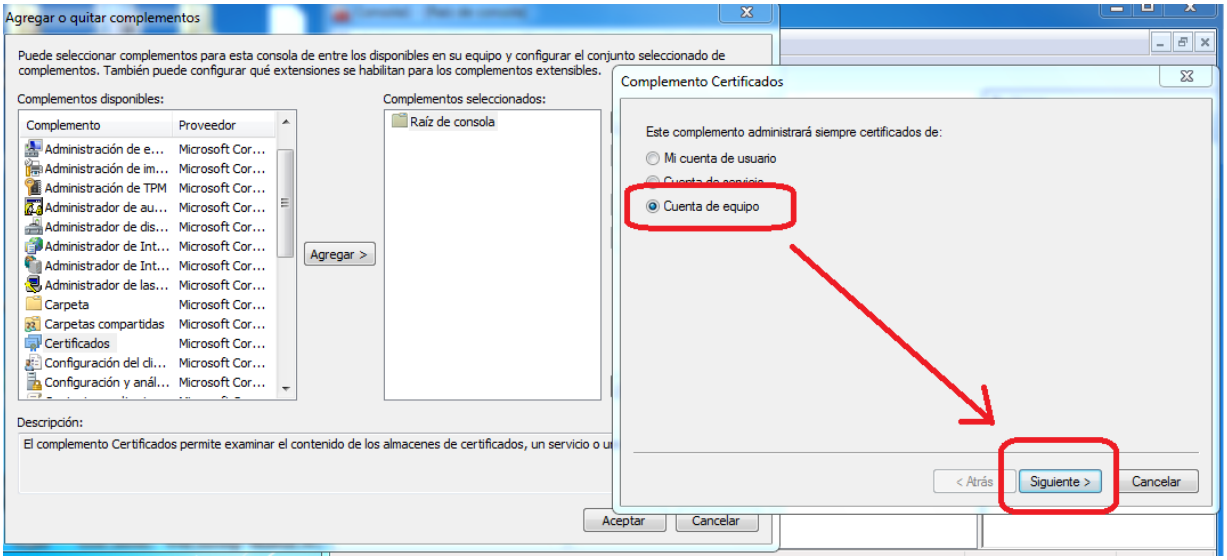
2.- Desde la nueva pantalla que se ha abierto seleccionaremos “/Archivo/Agregar o quitar complemento” que nos abrirá una nueva pantalla emergente.

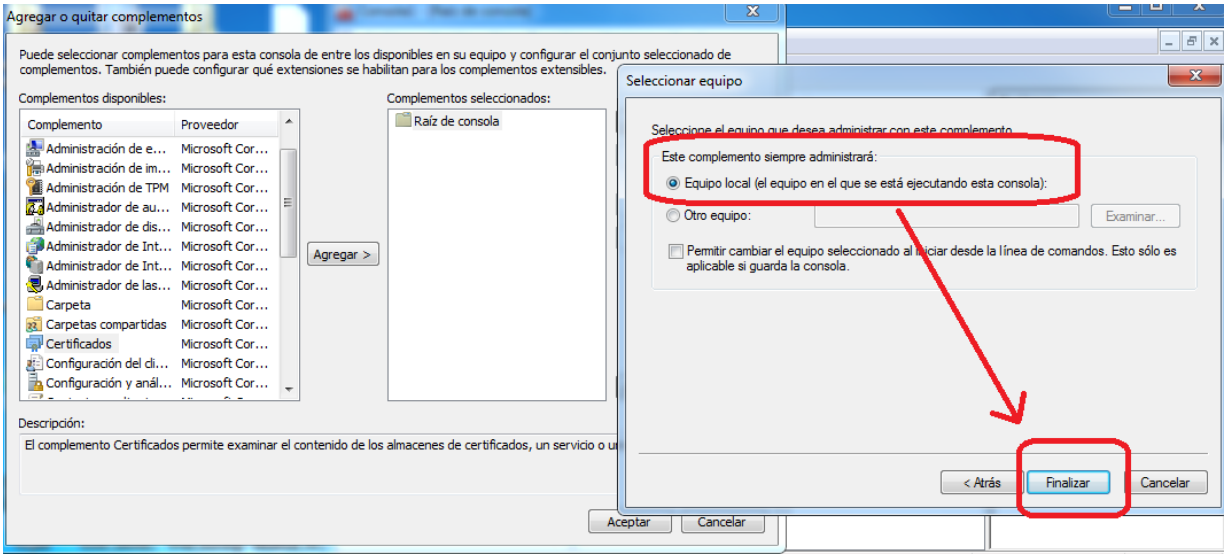


3.- Desde esta nueva pantalla seleccionaremos “Certificados” y le daremos al botón “Agregar”.

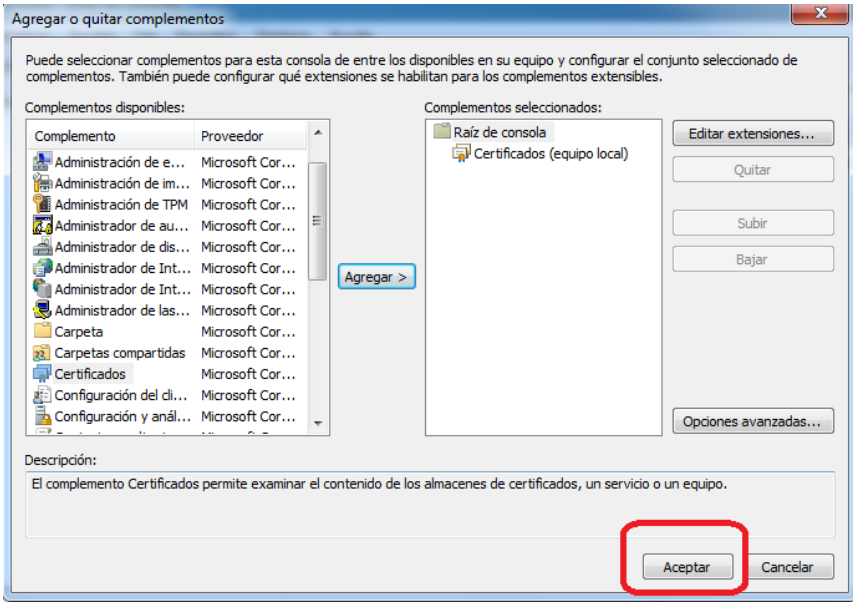


4.- Después seleccionaremos “Cuenta de equipo” y finalmente “Equipo local”.

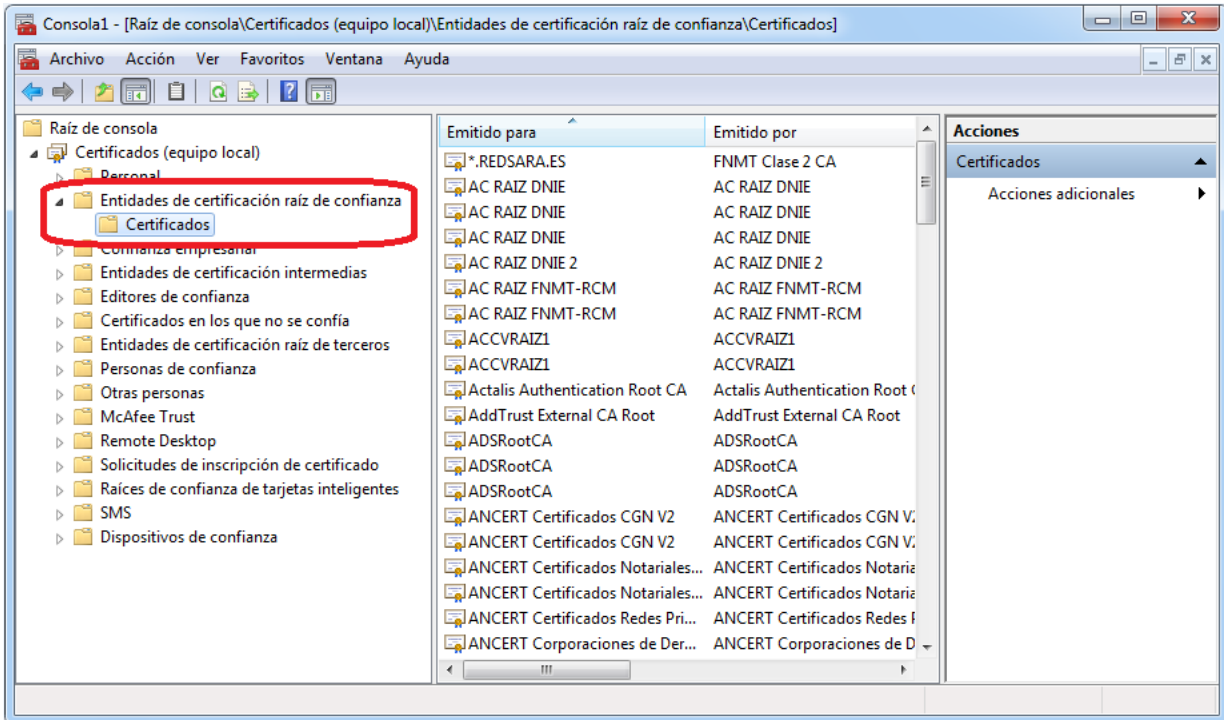




5.- Para finalizar, le daremos al botón “Aceptar” en nuestra pantalla inicial, y esto nos abrirá la gestión de los certificados de nuestro equipo.



6.- Desde la gestión de certificados de nuestro equipo (que vemos bajo) se realizará la importación del certificado. El certificado generado por el Registro Electrónico y que deberemos importar se encontrará en una ruta similar a esta "D:\Usuarios\mmelendo\.jappsrv\jappsrv.cer", donde "mmelendo" es el usuario identificado en esa máquina. Para importarlo, tendremos que darle al botón derecho de la carpeta "Certificados" que está dentro de "Entidades de certificación raíz de confianza". Una vez hecho esto, seleccionaremos "Todas las tareas >> Importar". Finalmente seleccionamos el certificado que queremos importar y aceptamos.



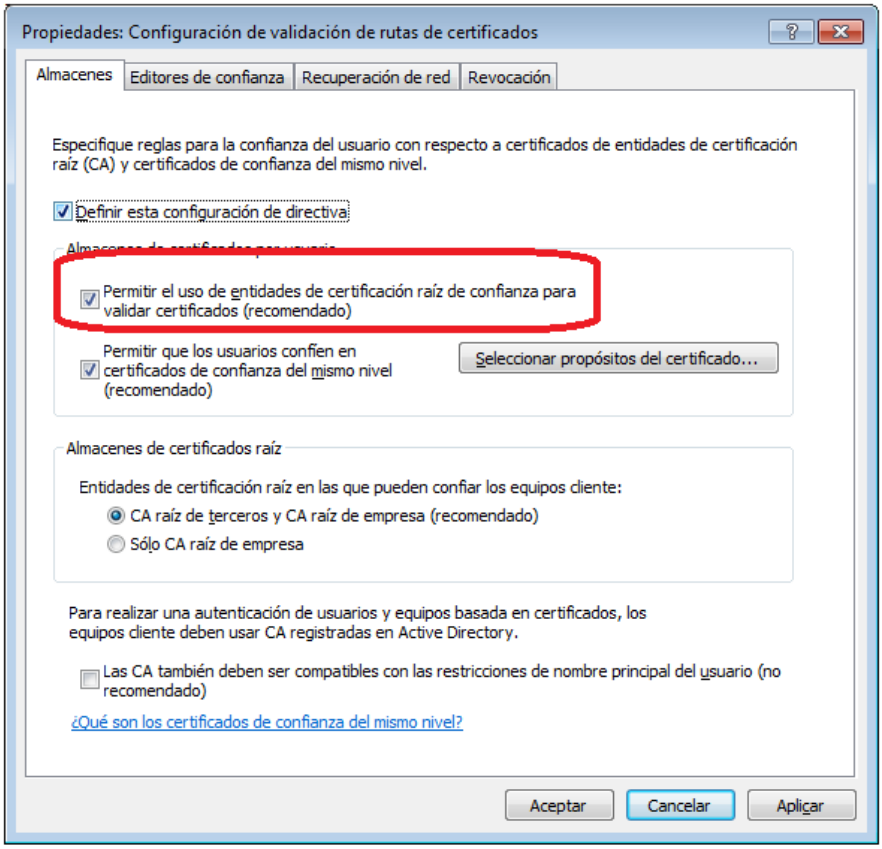
7.- El último paso sería ir de nuevo al navegador y comprobar de nuevo, como se ha indicado en el punto 1.4 de este documento, que el certificado se ha instalado correctamente.

1.6 Acceso de usuarios de dominio

En el caso en que un usuario de dominio esté intentando acceder al Registro Electrónico o las Notificaciones Electrónicas se tendrán que revisar los siguientes puntos.

1.6.1 Instalación de certificados raíz de confianza

Se deberá comprobar que los usuarios de dominio deben de poder instalar certificados raíz de confianza. Para comprobar si esto es posible un administrador del dominio deberá ejecutar desde una consola de Windows el comando "gpedit.msc" (sin las comillas). Desde ahí se seleccionarán las siguientes opciones "Configuración de equipo >> Configuración de Windows >> Directivas de clave pública >> Configuración de rutas de certificados". Esto abrirá la pantalla que puede verse bajo. Para que se permita la instalación de certificados raíz de confianza debe estar marcado el check que aparece señalado. En el caso de que NO se quiera activar esta opción, cada usuario del dominio debería instalarse manualmente las claves públicas tal y como se ha explicado en el punto 1.4.1.



1.6.2 Permisos restringidos

Hay que comprobar que los usuarios de dominio con los que se está intentando realizar los trámites tengan permiso de escritura en C:\Users\usuario\AppData\Local\Temp

1.7 Proxy

Si se está utilizando un proxy para establecer la conexión a internet es muy probable que todas las conexiones, incluida la 127.0.0.1 intenten pasar por él. Si se usa un script para detectar si determinadas IPs o direcciones han de salir por el proxy, hay que configurarlo para que NO use el proxy la dirección local 127.0.0.1

1.8 Problemas de tramitación con Windows 10

A continuación se detallan algunos problemas que pueden surgir al tramitar con Windows 10 y cómo solucionarlos.

1.8.1 Windows Defender

Windows Defender es el antivirus y cortafuegos que viene por defecto en Windows 10. Si se tiene activo este antivirus es muy probable que no le permita ejecutar el applet del Registro Electrónico. Es por ello que debe de añadirse una excepción en el antivirus para permitir la tramitación, o como medida temporal, desactivarlo durante este proceso para volverlo a activar tras su finalización.

Lo que se acaba de comentar también puede suceder con otro tipo de antivirus pero es menos probable.

1.8.2 Ejecución de Internet Explorer como administrador

Otro problema que puede darse en Windows 10 es que no tenga los privilegios suficientes de usuario. Para evitar este problema, hay que ejecutar Internet Explorer como administrador. Para ello, nos colocaremos sobre el icono de Internet Explorer y manteniendo la tecla de las mayúsculas presionadas (Shift), le daremos al botón derecho del ratón para seleccionar “Ejecutar como Administrador”.

2 Windows – Firefox

2.1 Versiones navegador

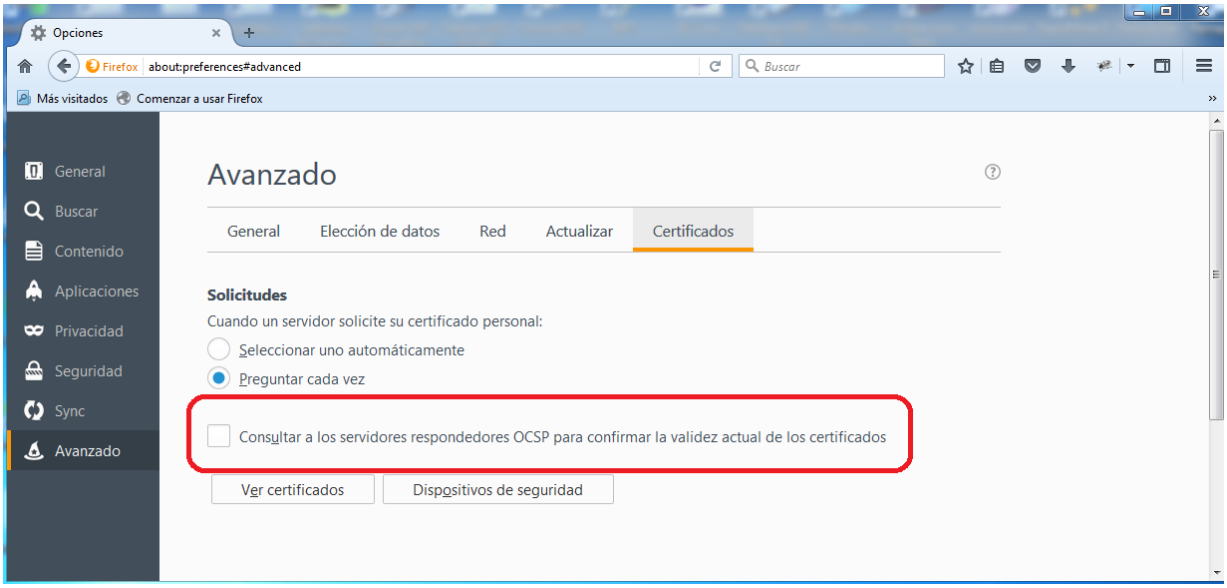
Las versiones de Firefox soportadas son la 42 o superior.

2.2 Claves públicas

Firefox dispone de un almacén de certificados distinto al de Internet Explorer y Chrome. Es por ello, que tanto el certificado que se quiera utilizar como las claves públicas del mismo deberán estar instaladas en el almacén de claves de Firefox. Adicionalmente, **y aunque no se realice la tramitación desde Internet Explorer**, deben añadirse las claves públicas del certificado que queramos utilizar en él, o desde al almacén de Windows. Si no se incluyen, cuando vayamos a firmar una solicitud de Registro Electrónico (durante el paso 2 de la tramitación), el desplegable que muestra el certificado con el que vamos a firmar aparecerá vacío.

2.3 OCSP

Revisar que dentro de las opciones de Firefox NO está marcada la opción de "Consultar a los servidores respondedores OCSP para confirmar la validez actual de los certificados" tal y como puede verse en la imagen de bajo.



2.4 Instalación del certificado del applet

Para el correcto funcionamiento del Registro Electrónico y las Notificaciones Electrónicas, habría que comprobar si el certificado del applet de firma se ha instalado correctamente en el navegador. Para ello tendríamos que dirigirnos a las opciones de Firefox, "/Opciones/Avanzado" y seleccionar la pestaña "Certificados". Una vez allí haremos clic sobre el botón "Ver certificado" y buscaremos el certificado del applet dentro de la pestaña de "Autoridades", tal y como puede verse en la imagen de bajo. En el caso de que el certificado no se haya instalado o se haya instalado en otra pestaña distinta a la indicada, tendremos que realizar la instalación del certificado manualmente. Para ello y desde la página que acabamos de comentar, hacemos clic en "Importar", seleccionaremos el certificado del applet y aceptaremos la importación del mismo. Normalmente el certificado se encontrará en una ruta similar a esta "D:\Usuarios\mmelendo\.jappsrv\jappsrv.cer", donde "mmelendo" es el usuario identificado en esa máquina.