Ayuntamiento de Logroño

Servicio de Informática y Nuevas Tecnologías
Avenida de la Paz, 11
26071 – Logroño (La Rioja)

Aspectos relacionados con los certificados digitales en la Sede Electrónica del Ayuntamiento de Logroño.

Ayuntamiento de Logroño

Contenido

1. Introducción

En la sede electrónica del Ayuntamiento de Logroño existen diferentes aspectos relacionados con la firma electrónica, como son:

- Identificación de la sede y establecimiento de conexiones seguras.
- Identificación del ciudadano para el acceso a la parte privada de la sede electrónica mediante certificado digital.
- Firma de Solicitudes.
- Validación de la firma electrónica incluida en los acuses de recibo generados por el Ayuntamiento.

En el presente documento se tratan los puntos anteriores y se indican los requisitos de configuración que deben verificar los equipos de los ciudadanos.

2. Sede electrónica del Ayuntamiento de Logroño y certificado de Sede

La Ley 40/2015 de Régimen Jurídico del Sector Público, define la sede electrónica como aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias. Así mismo se establece que las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.

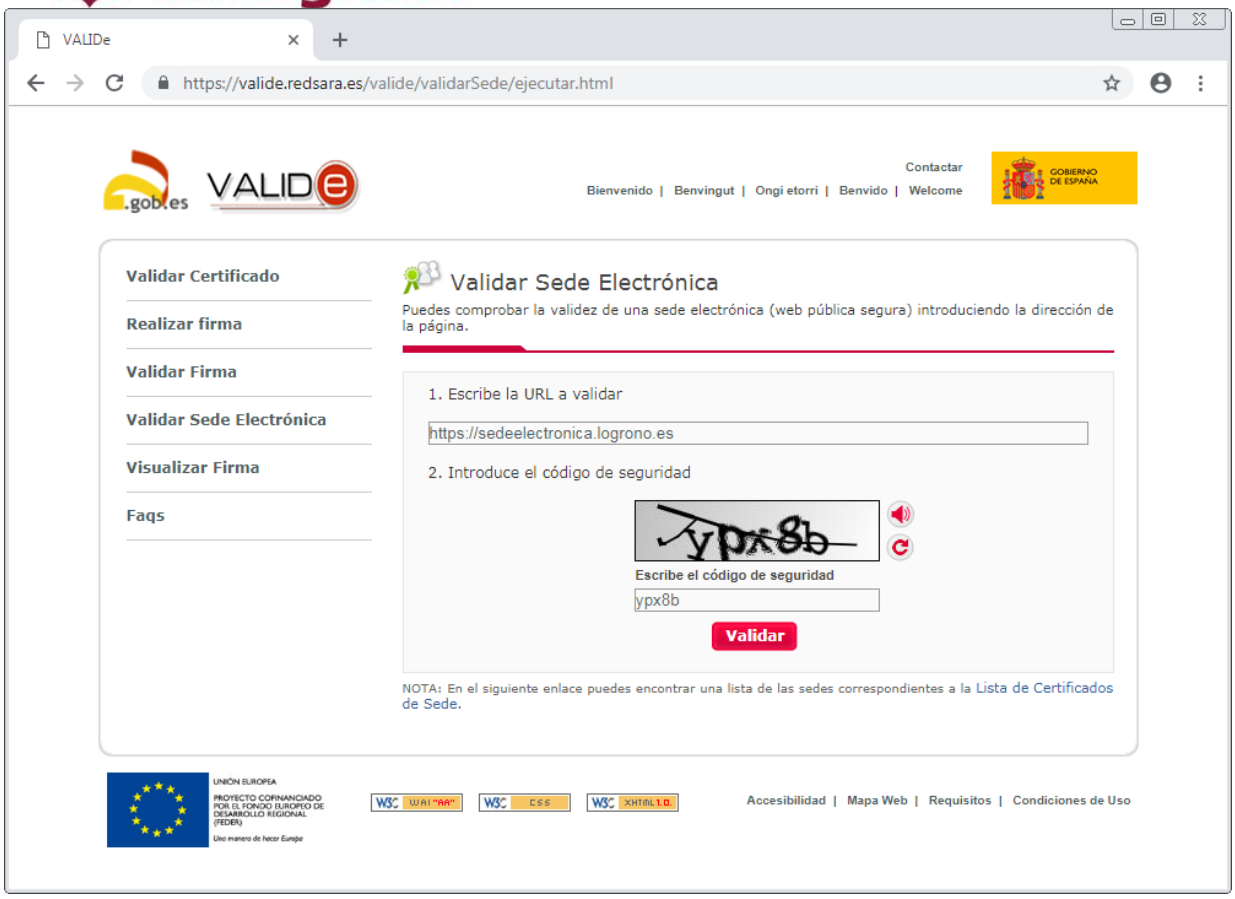
2.1 Certificado de Sede Electrónica

La autenticidad de la sede electrónica del Ayuntamiento de Logroño está garantizada mediante un certificado digital emitido por la Autoridad de Certificación Firmaprofesional – Secure Web 2021. Esta autoridad de certificación ha sido habilitada por AC Firmaprofesional S.A. como Autoridad de certificación subordinada de la Autoridad Raíz.

2.2 Verificación de la autenticidad de la sede

Para comprobar la validez de cualquier sede electrónica y por tanto también la del Ayuntamiento de Logroño, puede acceder a la página web https://valide.redsara.es que el Gobierno de España pone a disposición de los ciudadanos para tal fin. En esta página se accederá a la opción *Validar Sede Electrónica*.

En la ventana que se presenta se introducirá la dirección de la sede electrónica del Ayuntamiento de Logroño (*https://sedeelectronica.logrono.es*), el código de seguridad y se pulsará el botón *Validar*.



3. Acceso a la sede electrónica mediante certificado digital

La sede electrónica permite interactuar de forma telemática con el Ayuntamiento de Logroño tanto para la realización de distintos trámites como para la consulta del estado de tramitación. La Sede, se encuentra estructurada en dos zonas diferenciadas:

*** Zona Pública**
A esta zona se puede acceder sin necesidad de que el ciudadano o la empresa (en adelante referidos como usuario) necesite acreditarse y en la que se dispone de diferentes servicios como información general del funcionamiento de la sede, servicios de Contratación, servicio de verificación de documentos, lectura de contadores de agua, etcétera.

*** Zona Privada**
En esta zona de la Sede, se podrá llevar a cabo la tramitación electrónica de una serie de procedimientos, así como la realización de consultas de aquellos expedientes reales correspondientes a los usuarios autenticados. En esta zona de la Sede Electrónica se podrán realizar trámites como Solicitudes de Devoluciones de Ingresos Indebidos, gestión de Domiciliaciones Bancarias, cambios del Domicilio de Notificación, solicitudes de certificados y volantes de Empadronamiento, creación de Autodeclaraciones, etc.

El acceso a la zona privada de la sede se realizará mediante el uso de certificados electrónicos admitidos por el Ayuntamiento de Logroño o mediante acreditación de usuario y contraseña otorgadas por el Ayuntamiento. En el apartado Seguridad y Privacidad / Sistemas de firma admitidos se indican los distintos tipos de certificado que pueden utilizarse para la conexión a la Sede. Por otro lado, se debe tener en cuenta que parte de los trámites requieren el uso de

certificados electrónicos independientemente de que la conexión a la sede se realice mediante usuario y contraseña.

4. Firma de Solicitudes

Parte de los trámites puestos a disposición de los ciudadanos en la sede electrónica requieren la firma digital del solicitante para dar por presentada la solicitud. Esto garantizará la integridad y no repudio de la misma.

La firma digital se realiza en el equipo del ciudadano que va a realizar la firma. El proceso de firma se basa en la aplicación *AutoFirma*.

AutoFirma es una aplicación, generada por el Gobierno de España, que debe descargarse e instalarse en el equipo con carácter previo a la primera vez que se utilice la firma. Para la descarga e instalación de AutoFirma se seguirá lo indicado en la sección *Configuración para permitir la ejecución de la Aplicación AutoFirma*.

A continuación se muestra la matriz de compatibilidad como un cruce entre sistemas operativos, navegadores y las alternativas de firma disponibles para cada uno.

El carácter (-) marca combinaciones que técnicamente no son viables, como por ejemplo el navegador Safari en MS Windows.

Entorno	Mozilla Firefox 27+ ***	Google Chrome 41+	MS Internet Explorer* 10+	MS Edge 25+	Safari 9.1+
Windows 8+ y Windows 10	OK	OK	OK	OK	-
Windows 7	OK	OK	OK	OK	-
Ubuntu Linux 14.04.5+	NO**	OK	-	-	-
Apple OS X 9.1+	-	-	-	-	OK

* No aplica sobre la distribución para el entorno Metro de MS Internet Explorer en Windows 8+.
** En Ubuntu Linux 14.04.5 es posible usar AutoFirma con Firefox, siempre y cuando se logre configurar correctamente el acceso de AutoFirma al almacén de certificados de Firefox.
*** Se recomienda actualizar a la última versión disponible o en su defecto instalar una inferior a la 42.0.

4.1. Configuración para permitir la ejecución de la aplicación AutoFirma

AutoFirma es una herramienta de escritorio con interfaz gráfica, proporcionada por el Gobierno de España, que permite la ejecución de operaciones de firma de ficheros locales y formularios en entornos de escritorio (Windows, Linux y Mac OS X). Esta aplicación debe descargarse e instalarse en el equipo con carácter previo a la primera vez que se requiera la firma.

Para la instalación de Autofirma se accederá a http://firmaelectronica.gob.es/Home/Descargas.html. En esta página se procederá a la descarga de Autofirma correspondiente al sistema operativo del equipo en el que se va a instalar. El fichero descargado incluye un instalador integrado y un manual de instalación "AF_manual_instalacion_y_gestion_ES" que describe los pasos de instalación de Autofirma.

Se debe tener en cuenta que aunque en el documento "AF_manual_instalacion_y_gestion_ES" no se especifica como requisito disponer de ninguna versión de java, se ha comporbado que al

menos en la versión 1.4.3 de AutoFirma, se requiere tener instalado un entorno de ejecución Java. Para conocer cual es la versión de java que se tiene instalada en el equipo se puede acceder a la url http://www.java.com/es/download/installed.jsp. En esa página pulsar sobre el botón “Verificar la versión de Java”. Para actualizar la versión de la máquina virtual java del equipo se puede acceder a http://www.java.com/es/.

4.1.1. Requisitos Mínimos Entorno Cliente

Autofirma tiene los siguientes requerimientos en cuanto a entorno operativo:

Sistema operativo:

- Microsoft Windows 7 o superior.
  - Soportado directamente en 7, 8, 8.1 y 10.
  - En 32 o 64 bits.
- Apple OS X 10.11 o superior.
  - Soportado directamente en 10.11 y 10.11.1.
- Linux
  - Guadalinex, Ubuntu.

Navegadores Web (para la invocación por protocolo)

- Microsoft Windows
  - Google Chrome 46 o superior.
  - Mozilla Firefox 41.0.1 o superior.
  - Microsoft Internet Explorer 11 (no se admiten los modos de compatibilidad con versiones anteriores, ni ninguna otra versión anterior).
  - Microsoft Edge v20.
- Linux
  - Mozilla Firefox 41.0.1 o superior.
- Apple OS X
  - Apple Safari 9.0 o superior.

En Linux se necesita un entorno de ejecución de Java de Oracle u OpenJDK (marcado como dependencia en el instalador integrado de AutoFirma).

4.1.2. Notas Importantes referentes a la Instalación de AutoFirma

4.1.2.1. Verificación de la instalación del certificado AutoFirma ROOT

Para garantizar que la instalación de AutoFirma se ejecutó correctamente se debe verificar la instalación del certificado AutoFirma ROOT.
Es importante mencionar los siguientes puntos para que se lleve a cabo la correcta instalación de AutoFirma y del certificado:

- Como se ha indicado anteriormente, es necesario que se encuentre instalado el JRE (Java Runtime Environment) que corresponda según el Sistema Operativo.

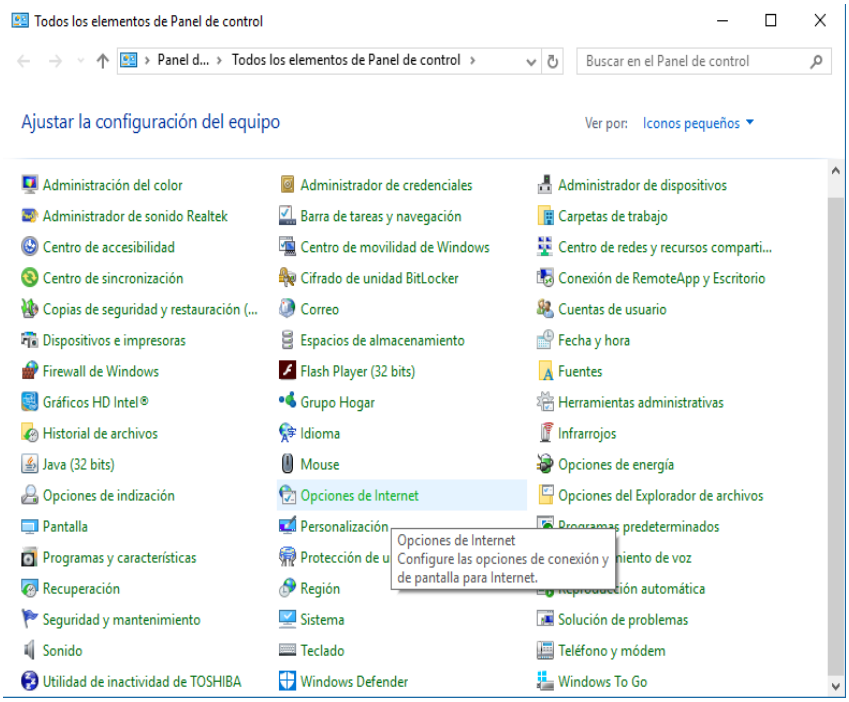
- Es necesario que los navegadores se encuentren cerrados.

A continuación se listan los pasos para verificar la instalación del certificado AutoFirma ROOT tanto en Windows como en Macintosh. Para los demás sistemas operativos y navegadores no mencionados los pasos a seguir son similares:

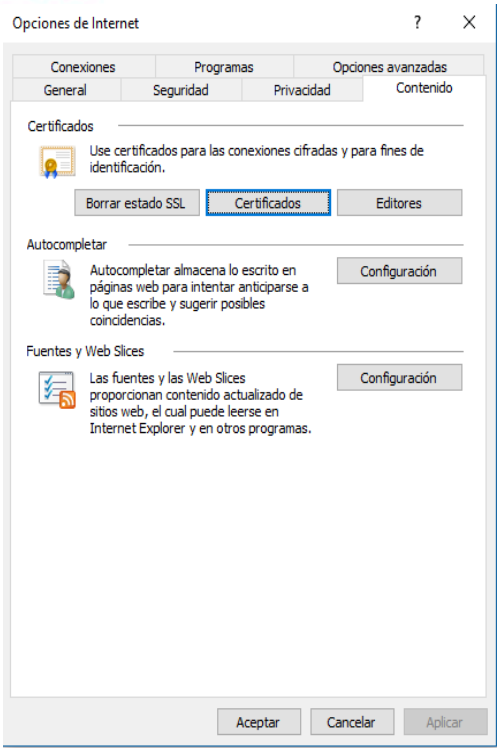
Windows

- Windows + navegadores Internet Explorer, Edge y Google Chrome:

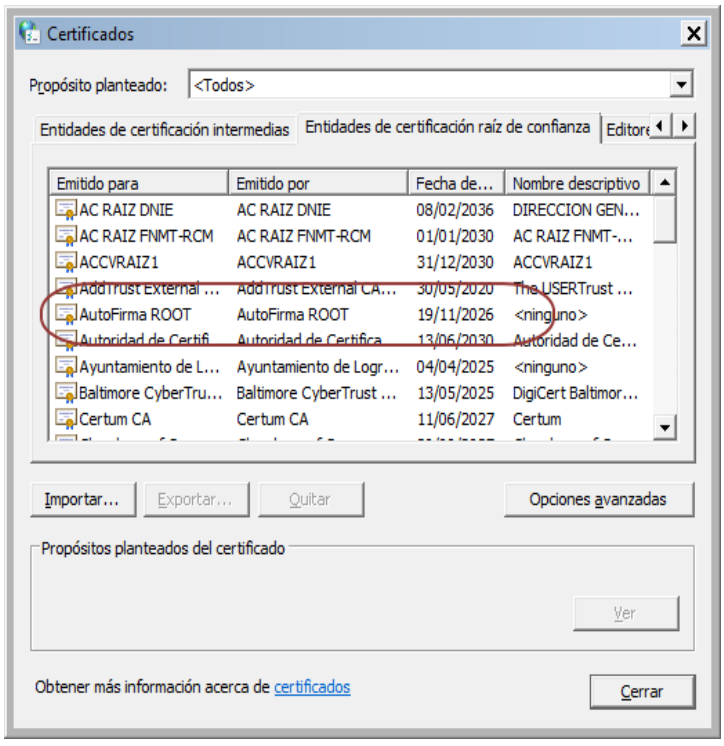
Ir al Panel de Control en Windows según corresponda. Seleccionar la opción “Opciones de Internet”:



Ahí, seleccionar la pestaña “Contenido” y dar clic sobre el botón “Certificados”:



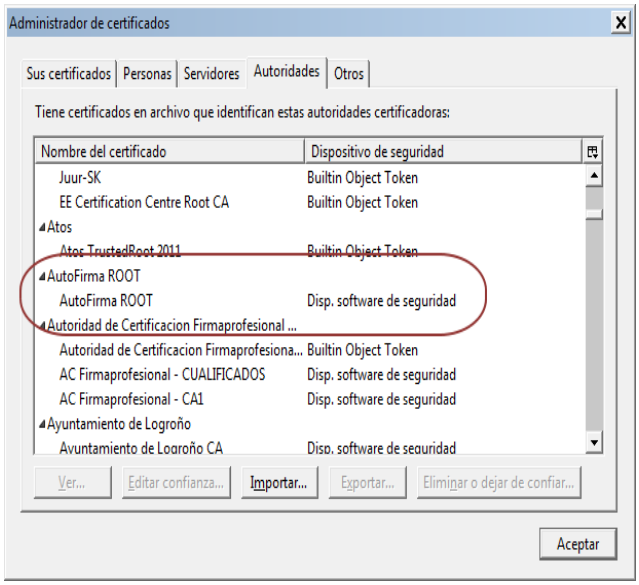
Ir a la pestaña "Entidades de certificación raíz de confianza" y verificar que se encuentra instalado el certificado AutoFirma ROOT:



- Windows + Navegador Mozilla Firefox:

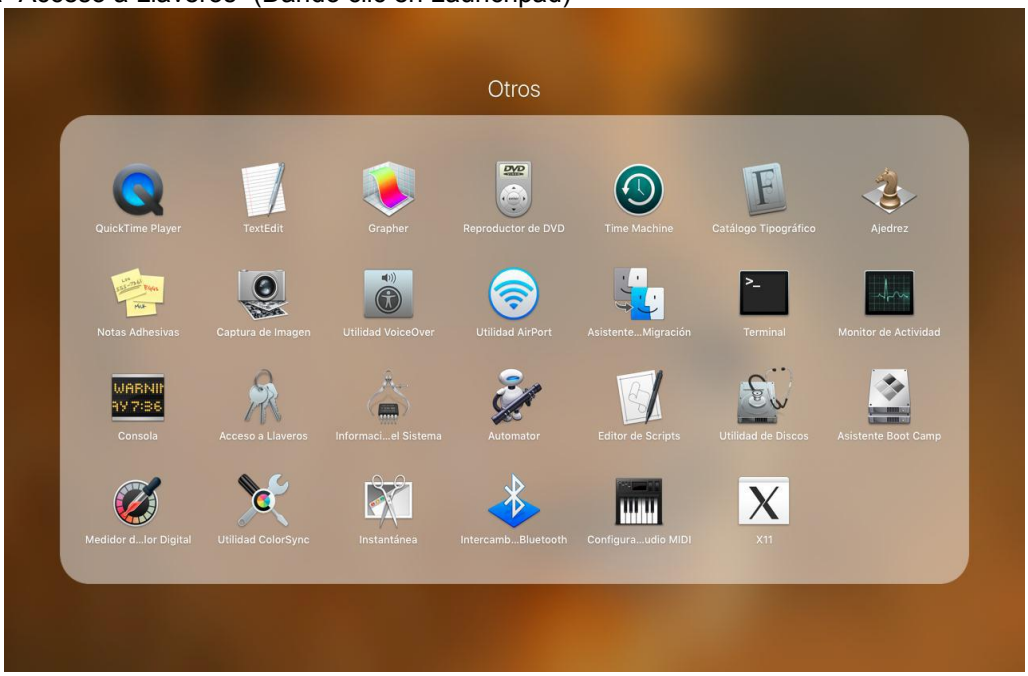
Como se ha indicado anteriormente Mozilla Firefox maneja su propio almacén de certificados,

los pasos a seguir para validar la instalación del certificado AutoFirma ROOT son los siguientes:
- Desde el Menú del navegador, seleccionar “Opciones”.
- Allí, seleccionar la opción “Avanzado” y dentro de esta la pestaña “Certificados”. Pulsar el botón “Ver Certificados”
- Seleccionar la pestaña “Autoridades” y verificar que se encuentre instalado el certificado AutoFirma ROOT:

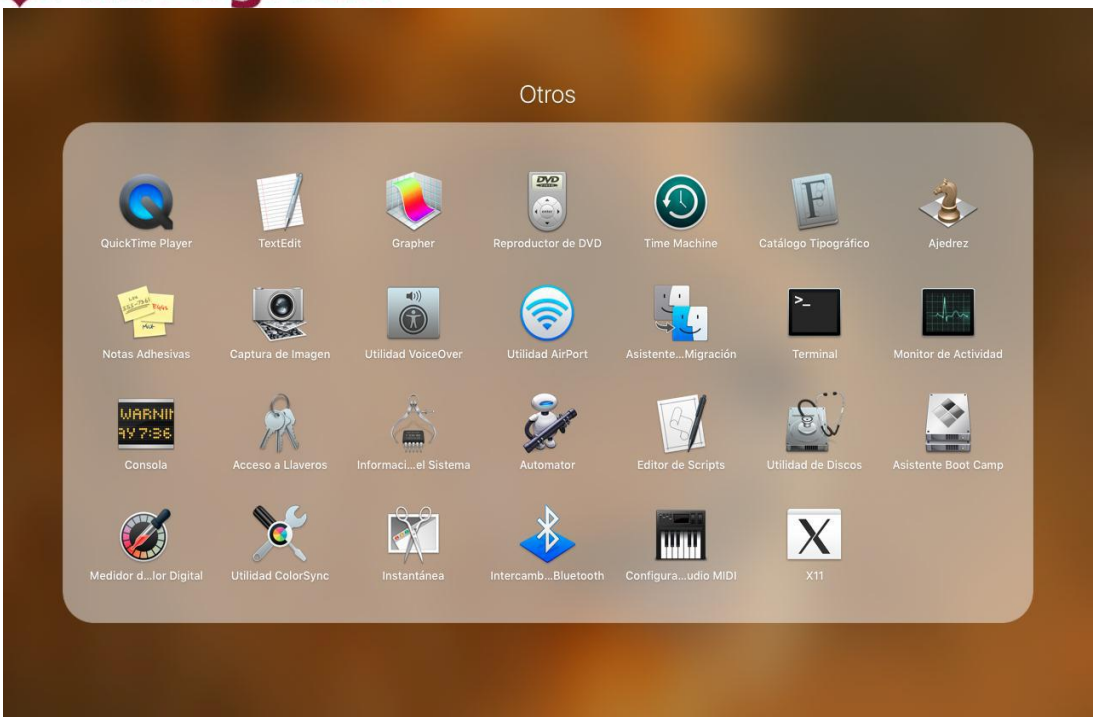


Macintosh

- Ir a “Acceso a Llaveros” (Dando clic en Launchpad)



En “Acceso a Llaveros”, seleccionar la opción “Sistema” y verificar que se encuentre instalado el certificado AutoFirma ROOT:



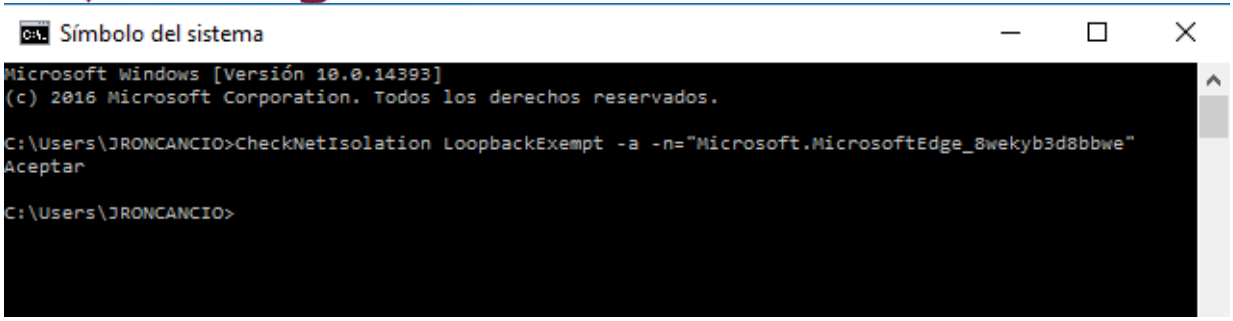
4.1.2. No permitir la ejecución del MiniApplet

En el momento de realizar la firma, se debe tener en cuenta que según la configuración del sistema del usuario puede aparecer en el navegador (navegadores que permitan la ejecución de Applets de Java) la siguiente advertencia de seguridad de Ejecución del MiniApplet:

Para evitar que se ejecute el MiniApplet y permitir que se ejecute la aplicación AutoFirma, si aparece el mensaje, pulsar el botón “Cancelar”.

4.1.3. Configuración del Navegador Microsoft Edge para que funcione con AutoFirma

Para que AutoFirma funcione correctamente en Microsoft Edge en Windows 10 se requiere ejecutar el siguiente comando en la terminal de Windows (Ejecutar como Administrador):
CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"

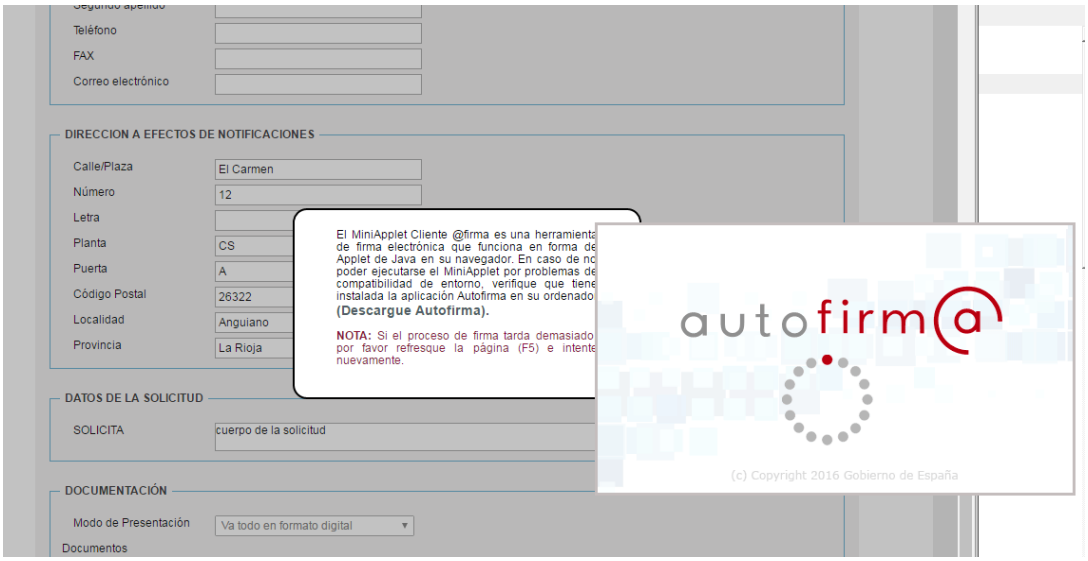


Este comando lo que hace es Habilitar el loopback en Microsoft Edge. Para más información al respecto puede consultar el siguiente link: https://www.ibm.com/support/knowledgecenter/en/SSPH29_9.0.3/com.ibm.help.common.infocenter.aps/r_LoopbackForEdge.html

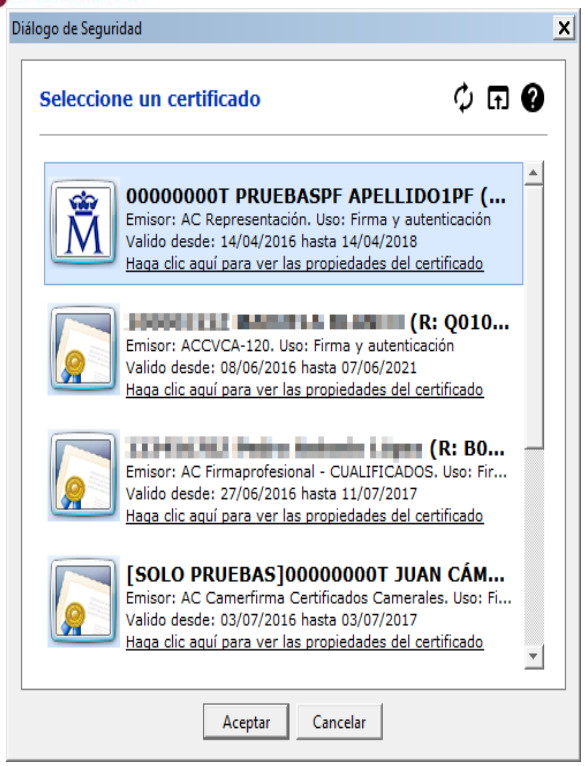
4.2. Pasos para firmar una solicitud

En los distintos trámites en los que se requiere la firma digital, se sigue un mecanismo similar en todos los trámites, que se describe a continuación.

Cuando se lance el proceso de firma se arrancará la aplicación AutoFirma que deberá estar instalada en el equipo como se ha indicado en este documento. Durante unos segundos se mostrará el logo de la aplicación AutoFirma.



A continuación se mostrará una lista con los certificados accesibles en el equipo.

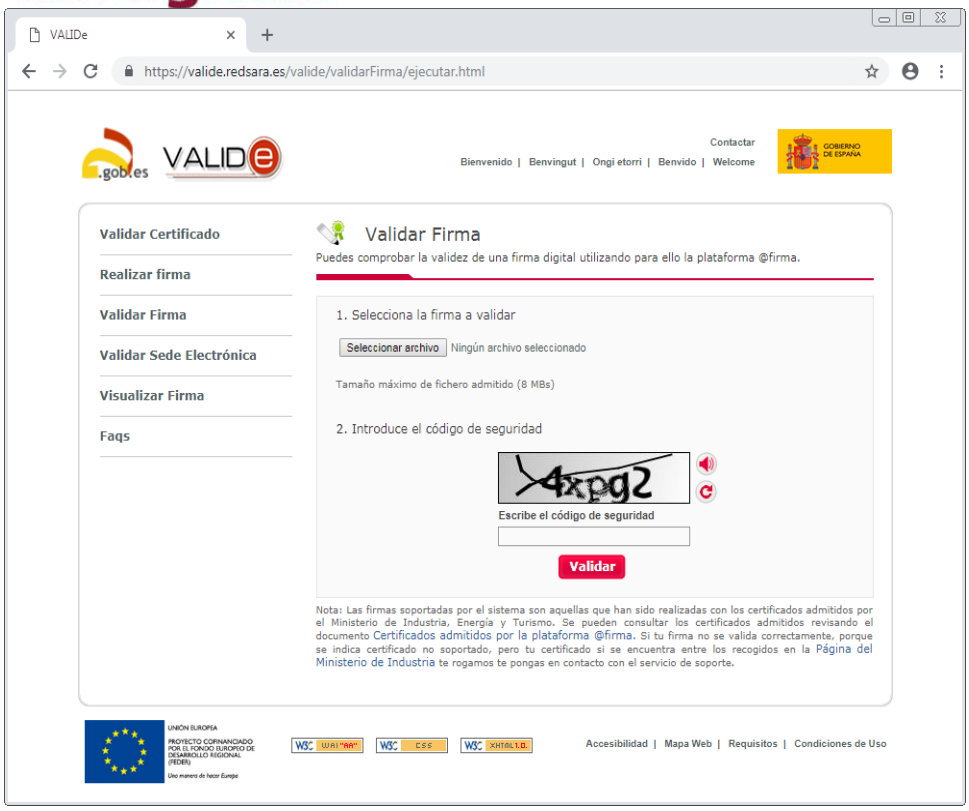


En la lista anterior se seleccionará el certificado con el que se quiere firmar la solicitud y se pulsará el botón Aceptar. Dependiendo de la configuración del equipo, para realizar la firma se puede pedir el pin del certificado, se puede mostrar un aviso solicitando permiso para acceder a un elemento protegido o directamente se puede proceder a la firma. Cuando finaliza la firma aparecerá un mensaje de confirmación. **Es muy importante tener el cuenta que el hecho que de la firma se haya realizado correctamente no supone que haya finalizado la presentación de la solicitud, ya que después de la firma se debe registrar en Registro General y emitir el justificante de presentación. La presentación se considerará realizada cuando se haya emitido el justificante de presentación.**

5. Validación de la firma digital incluida en los acuses de recibo generados por el Ayuntamiento de Logroño

Los trámites desplegados en la sede electrónica, que están relacionados con la presentación de solicitudes, emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación. Estos recibos estarán firmados con un certificado digital del Ayuntamiento de Logroño que garantiza la integridad y el no repudio de los documentos aportados

Para comprobar las firmas de estos acuses de recibo puede acceder a la página web https://valide.redsara.es que el Gobierno de España pone a disposición de los ciudadanos para tal fin. En esta página se accederá a la opción *Validar Firma*.



En esta ventana se seleccionará el archivo que contiene la firma, se introducirá el código de seguridad y se pulsará el botón *Validar*.