AYUNTAMIENTO
TRES CANTOS

1. REQUISITOS MÍNIMOS

El uso de AutoFirma como herramienta de firma integrada dentro del proceso de firma de trámites web tiene los siguientes requerimientos en cuanto a entorno operativo:

- Sistema Operativo
  - Microsoft Windows.
    - Soportado directamente en 7, 8, 8.1, 10 y 11
    - En 32 o 64 bits.
  - Linux:
    - Distribuciones probadas: Ubuntu, Fedora y OpenSuse.
  - Apple macOS:
    - Soportado directamente en Ventura, Monterey y Big Sur
- Navegadores Web
  - Microsoft Windows.
    - Google Chrome 46 o superior.
    - Mozilla Firefox 41.0.2 o superior.
    - Microsoft Edge 60 o superior (Edge Chromium)
    - Microsoft Internet Explorer 8 o superior
    - Microsoft Edge Legacy v20 o superior (EdgeHTML).
  - Linux:
    - Mozilla Firefox 41.0.1 o superior.
  - Apple macOS:
    - Apple Safari 12.0 o superior
    - Google Chrome 46 o superior.
    - Mozilla Firefox 65 o superior.

ADVERTENCIA: El funcionamiento de AutoFirma al invocarlo desde versiones de Internet Explorer anteriores a la 11 (o Internet Explorer 11 en modo de compatibilidad con una versión anterior) está supeditado a que el administrador de la aplicación web haya cumplido ciertos requisitos durante el despliegue. Para asegurar el correcto funcionamiento de las operaciones de firma online utilice otro de los navegadores soportados.

En entornos macOS y Windows no es necesario tener instalado un entorno de ejecución de Java.

En Linux se necesita un entorno de ejecución de Java 11 de Oracle u OpenJDK 11 (marcado como dependencia en el instalador integrado de AutoFirma).

Es obligatorio que AutoFirma sea instalado antes de iniciar el trámite web en el que se usará para ejecutar las operaciones de firma.

AYUNTAMIENTO
TRES CANTOS

2. CONFIGURACIÓN JAVA

Siga las recomendaciones de la página oficial: https://www.java.com/es/

Donde dispone de una guía en el siguiente enlace: https://www.java.com/es/download/manual.jsp

3. OPERACIONES TELEMÁTICAS CON DNIe

Página oficial: https://www.dnielectronico.es/

3.1 QUE HACE FALTA PARA UTILIZARLO

Siga las recomendaciones de la página oficial
https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_300

Requisitos técnicos
https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1009&id_menu=40

3.2 CONFIGURACIÓN EN EQUIPOS MAC

Siga las recomendaciones de la página oficial: https://www.dnielectronico.es/

Tal como indican, para poder interaccionar adecuadamente con las tarjetas criptográficas en general y con el DNI electrónico en particular, su equipo ha de tener instalados unas "piezas" de software denominadas módulos criptográficos.

En los entornos MacOS podemos utilizar el DNI electrónico a través de un módulo criptográfico denominado PKCS#11.

Software requerido para la instalación en sistemas Mac OS X 64 bits
http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1113

Manual Instalación y Configuración PKCS11 DNIe
https://www.dnielectronico.es/PDFs/manuales_instalacion_unix/Manual_de_Instalacion_de_MulticardPKCS11_DNIE.pdf

4. INSTALACIÓN Y CONFIGURACIÓN AUTOFIRMA

Siga las recomendaciones de la página oficial: https://firmaelectronica.gob.es/

Manual de Instalación para Usuarios (1.8.2 y siguientes)

https://administracionelectronica.gob.es/ctt/resources/Soluciones/138/Descargas/AF-manual-instalacion-usuarios-ES-1-8-2.pdf?idIniciativa=138&idElemento=11402

Tutoriales AutoFirma

https://firmaelectronica.gob.es/Home/Ciudadanos/Ciudadanos-Video-Firma

4.1 Verificación de la instalación

Puede realizar un test de verificación y firma con AutoFirma a través del siguiente enlace:

https://www.sededgsfp.gob.es/es/Paginas/TestAutoFirma .aspx

RECOMENDACIONES GENERALES

- Verificar los permisos del usuario: Es necesario asegurarse de que el usuario tenga permisos suficientes para acceder al almacén de certificados. Para hacer esto, se debe iniciar sesión con una cuenta de usuario con permisos de administrador.
- Desactivar el control de cuentas de usuario: El control de cuentas de usuario (UAC) de Windows puede causar problemas de permisos. Es recomendable desactivarlo temporalmente para realizar la operación de firma y luego volver a activarlo.
- Ejecutar AutoFirma como administrador: Para asegurarse de que AutoFirma tenga los permisos necesarios, se debe ejecutar el programa como administrador. Para hacer esto, se debe hacer clic con el botón derecho del ratón en el icono de AutoFirma y seleccionar «Ejecutar como administrador».
- Agregar excepciones a la configuración del firewall: Si se utiliza un firewall, es posible que esté bloqueando la conexión de AutoFirma al almacén de certificados. Es recomendable agregar excepciones a la configuración del firewall para permitir el acceso de AutoFirma al almacén de certificados.

5. AYUDA

5.1 Verificación del estado de su certificado digital con VALIDe

El proceso de comprobación de un certificado implica en primer lugar la obtención de los datos del certificado y en segundo lugar la consulta a un servicio denominado Autoridad de Validación (AV) obteniendo como resultado de esta consulta es el estado actual del certificado: activo o revocado mostrando simultáneamente los datos incorporados al certificado (nombre y apellidos del titular, número de DNIe, etc.).

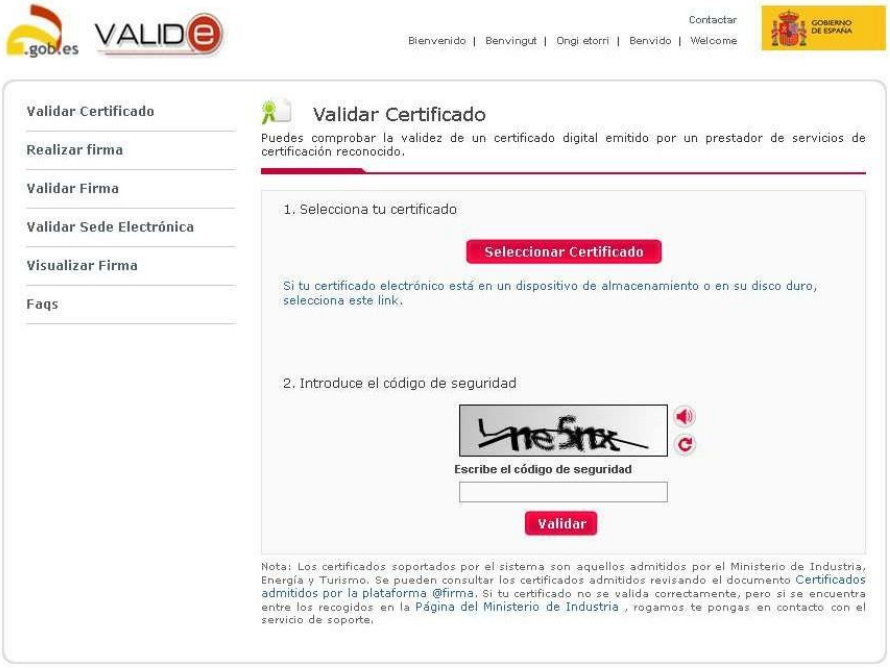
Para poder identificar el problema en el acceso al sistema con su certificado digital, necesitamos que se compruebe la validez del certificado con el que está accediendo al sistema en el servicio VALIDEe de la Administración General del Estado.

URL: https://valide.redsara.es/valide/

Tras haber accedido al enlace anterior, debe pulsar en el enlace “Validar Certificado” como se muestra en la siguiente imagen:

A continuación, en la siguiente pantalla debe seguir los pasos indicados en la misma:

1. Seleccionar el certificado que desee validar.
2. Introducir el código de seguridad de la imagen.
3. Pulsar en el botón “Validar”.



En caso de que el resultado de la validación del certificado **no sea correcto, se trata de un certificado no soportado** por el sistema y **debe acceder con otro certificado**.

Por el contrario, si el resultado de la validación **es correcto**, necesitamos la **clave pública del certificado** con el que está accediendo al sistema para tratar de identificar el problema y ofrecer una solución.