INSTRUCCIONES PARA EL USO DE CERTIFICADOS ELECTRÓNICOS PARA LA IDENTIFICACIÓN Y FIRMA ELECTRÓNICA EN LA SEDE ELECTRÓNICA DE LA AGENCIA ESTATAL DE SEGURIDAD AÉREA

Actualización de 12 de mayo de 2020

Las aplicaciones de la Sede Electrónica, para poder realizar operaciones de identificación y firma electrónica utilizando certificados electrónicos, han de utilizar el programa AutoFirma.

REQUISITOS TÉCNICOS DE LOS CERTIFICADOS ELECTRÓNICOS

El certificado electrónico que utilice para la firma ha de permitir realizar firmas electrónicas empleando los algoritmos SHA-2 y RSA. Si dispone de certificado en tarjeta criptográfica (por ejemplo, DNI electrónico o tarjeta criptográfica de la FNMT), debe asegurarse que tiene instalado en su equipo una versión del software que soporte los algoritmos anteriores.

- DNIe: soporta los algoritmos a partir de la versión 2.0
- FNMT: soporta los algoritmos a partir de la versión CERES v11.0.0 y TC-FNMT 2.0.0

Puede consultar la lista de certificados electrónicos soportados en la Sede Electrónica de AESA en el apartado “Relación de certificados electrónicos admitidos en esta Sede” situado en la página principal de la Sede Electrónica de AESA.

CONFIGURACIÓN PARA EL USO DE CERTIFICADOS ELECTRÓNICOS

Para poder realizar operaciones de identificación y firma electrónica con certificados electrónicos en la Sede Electrónica de AESA, su dispositivo debe tener instalada previamente la aplicación Autofirma. Además, debe permitir que el navegador pueda ejecutar la aplicación Autofirma cuando vaya a realizar estas operaciones.

Para más información sobre AutoFirma, consulte el manual de uso de AutoFirma disponible en el apartado “Información sobre navegadores y firma electrónica” de la Sede Electrónica.

CORREO ELECTRÓNICO:
cau.aesa@seguridadaerea.es

AVDA. GENERAL PERÓN, 40 1ª planta
28020 MADRID
TEL.: +34 91 396 8000

Tanto el navegador como AutoFirma tienen que configurarse para tener acceso al almacén de certificados de su dispositivo.

- Certificados software

  Deben estar importados en el almacén de certificados de su sistema operativo, o bien accesible desde las unidades o directorios de su dispositivo.

- Certificados en tarjeta criptográfica:

  Debe disponer de un lector de tarjeta compatible con su dispositivo, con los controladores (drivers) instalados para su correcto funcionamiento. Se recomienda tener la última versión disponible de los controladores.

  - DNIe: el servicio de actualización de Windows permite la instalación del controlador de manera automática al insertar el DNIe en su lector.

    No obstante, en algunos navegadores es necesaria la instalación del software proporcionado por la Dirección General de la Policía (esto es necesario en Mozilla Firefox).

  - FNMT: Ha de instalar el software TC-FNMT de funcionamiento de la tarjeta criptográfica en el dispositivo .

  En los manuales de instalación de cada prestador puede encontrar más información, así como los pasos a seguir y el software necesario para instalarlo en diferentes sistemas operativos.

PROBLEMAS CONOCIDOS RELACIONADOS CON EL USO DE CERTIFICADOS ELECTRÓNICOS

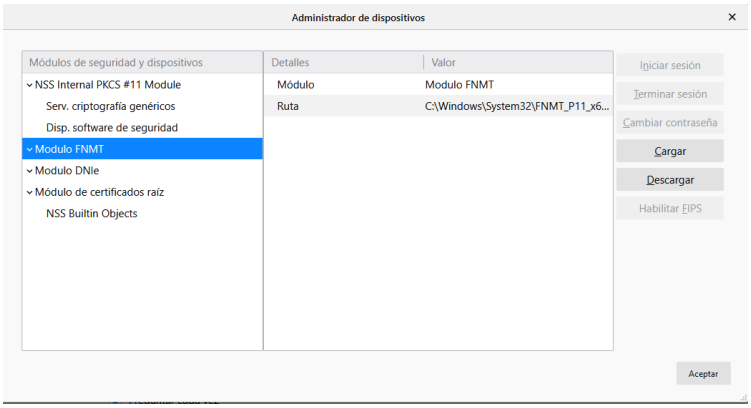
Existe una serie de problemas identificados relacionados con el uso de certificados electrónicos, que se enumeran a continuación:

- **No aparecen los certificados de la tarjeta criptográfica FNMT:** Compruebe que es un lector compatible y que está instalado el software proporcionado por el prestador FNMT.
- **No se accede al almacén de certificados de la tarjeta criptográfica FNMT/DNIe desde Mozilla Firefox:** El posible problema es que no tenga en el navegador configurado el módulo criptográfico que usa, por lo que instalando el software de la FNMT se podría solucionar si no lo tiene o volviéndolo a instalar en caso de que lo tuviera.

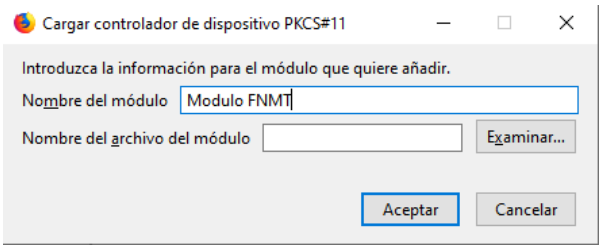
  Al realizar la instalación del software de la FNMT, comprueba si está instalado el navegador Mozilla Firefox en el sistema operativo, en el caso de que estuviera, lo configura para acceder a la tarjeta de la FNMT. (Para su correcta instalación debe estar cerrado el navegador).

  Aun así, se puede configurar el navegador de manera manual si ya tiene instalado el software, para ello abra el navegador Mozilla Firefox y en el apartado del menú de la barra de herramientas,

seleccione opciones , en la pestaña marque “Privacidad & Seguridad” y posteriormente acceda a “Dispositivos de seguridad”, compruebe que no tenga el módulo de la FNMT en el listado.

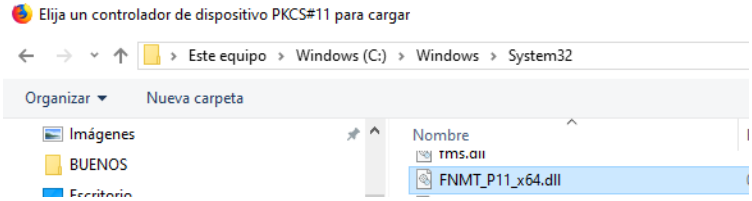


En el caso que no estuviera en la lista pulse “Cargar”, indíquele un nombre al módulo (Por ejemplo, Modulo FNMT) y buscamos el fichero **FNMT_P11.dll** en la ruta C:\Windows\System32 y pulsamos aceptar.



En el caso del DNIe si se tuviera el mismo problema que el anterior, la solución sería la misma, salvo que en la configuración manual, el fichero a buscar en C:\Windows\System32, se llama **DNIe_P11.dll**.

NOTA: Para sistemas de 64 bits los ficheros de la FNMT y DNIe respectivamente son **FNMT_P11_x64.dll** y **DNIe_P11_x64.dll**.



Para versiones anteriores del módulo criptográfico del DNIe los archivos a seleccionar son dos: **DNIe_P11_priv.dll y DNIe_P11_pub.dll**.

ENLACES PARA DESCARGAS

- AutoFirma de @firma

http://firmaelectronica.gob.es/Home/Descargas.html

- DNI electrónico

  http://www.dnielectronico.es/PortalDNIe/

- Tarjetas criptográficas FNMT

  https://www.sede.fnmt.gob.es/descargas/descarga-software

- Oracle Java

  https://www.java.com/es/download/