SISTEMA DE TRAMITACIÓN ELECTRÓNICA DEL FONDO DE GARANTIA SALARIAL

MANUAL DE USUARIO

VALIDACIÓN DE CERTIFICADOS Y FIRMAS ELECTRÓNICAS

SUMARIO

1 ACCESO AL SISTEMA Y OPERATIVA GENERAL 3

1.1 ENTRADA A LA APLICACIÓN 3

1.2 REQUISITOS TÉCNICOS DE LA APLICACIÓN WEB 3

1.2.1 REQUISITOS TÉCNICOS VALIDACIÓN DE CERTIFICADOS 3

1.2.2 REQUISITOS TÉCNICOS VALIDACIÓN DE FIRMAS 4

2 OPERATIVA WEB DEL SISTEMA 7

2.1 IMPLEMENTACIÓN DEL INTERFAZ WEB 7

2.1.1 VALIDAR CERTIFICADO 7

2.1.2 VALIDAR FIRMA 10

2.1.3 VALIDAR SEDE ELECTRÓNICA 12

1 ACCESO AL SISTEMA Y OPERATIVA GENERAL

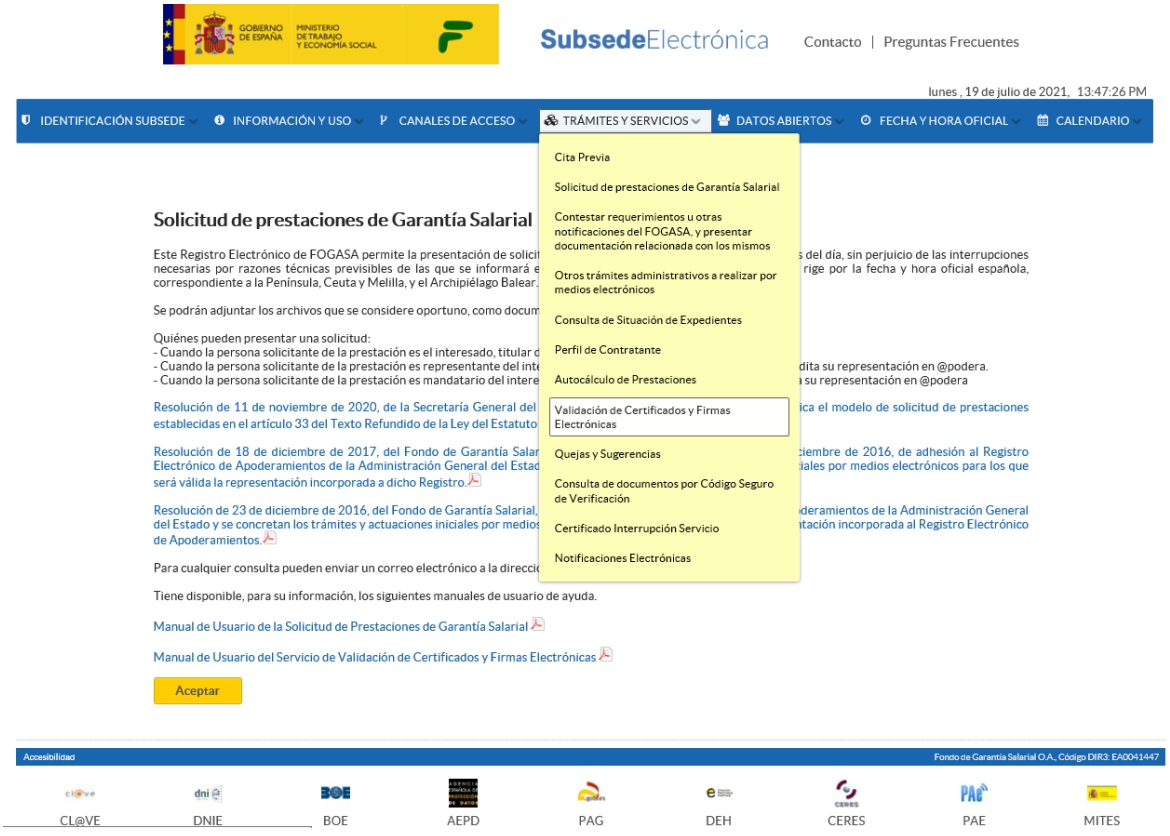
1.1 ENTRADA A LA APLICACIÓN

El acceso a la aplicación se realiza a través de un navegador web; preferiblemente Microsoft Internet Explorer o Mozilla Firefox.

Una vez abierto el navegador se introduce la siguiente dirección para el Sistema de Validación de Certificados y Firmas Electrónicas.

https://sede.fogasa.mites.gob.es/SEDE

Los/as usuarios/as accederán automáticamente a la página inicial:



Seleccionamos del menú **TRÁMITES Y SERVICIOS** la opción **Validación de Certificados y Firmas Electrónicas**

1.2 REQUISITOS TÉCNICOS DE LA APLICACIÓN WEB

A continuación se muestran los requisitos técnicos de los diferentes módulos del Sistema.

1.2.1 REQUISITOS TÉCNICOS VALIDACIÓN DE CERTIFICADOS

Los certificados admitidos deberán ser emitidos por alguna de las siguientes autoridades de servicio de certificación reconocida por @firma del MINHAFP.

La plataforma @firma admite certificados digitales reconocidos conforme el estándar ITU-T X.509 v3, emitidos por múltiples prestadores de servicios de certificación. Todos los prestadores se encuentran inscritos en el registro de la Secretaria de Estado de Telecomunicaciones y para la Sociedad de Información del Ministerio de Industria, Turismo y Comercio de autoridades conforme a lo establecido en el artículo 30 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

De acuerdo con la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) y la Ley 59/2003, de Firma Electrónica, los tipos de certificados admitidos son: certificado de persona física, certificado de persona jurídica, certificado de sello electrónico para la actuación automatizada, certificado de sede electrónica administrativa y certificado de empleado público. Cada uno de los certificados emitidos conllevará un grado de confianza asociado a los diferentes niveles de aseguramiento bajo los que se emitan, debido a los requisitos técnicos y de seguridad que estos niveles llevan asociados.

Puede ver los proveedores de certificación soportados por la plataforma @firma en la sección de la iniciativa en el Portal de Administración Electrónica.

1.2.2 REQUISITOS TÉCNICOS VALIDACIÓN DE FIRMAS

Las firmas admitidas en el Sistema de Validación de Firmas son aquellas generadas con el cliente de firma proporcionado por @firma y en formato XAdES, siendo posible validar los formatos avanzados:

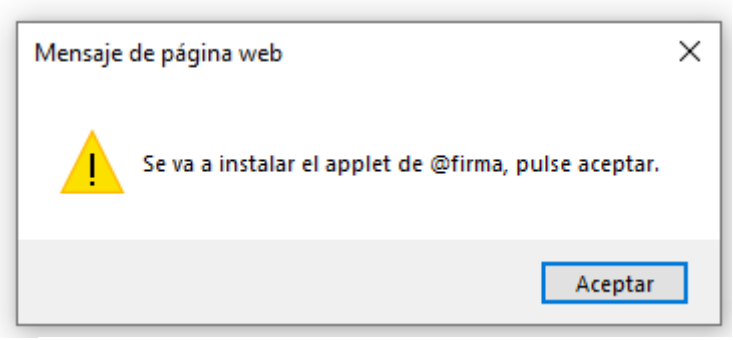
- XAdES
- XAdES-T
- XAdES-C
- XAdES-X
- XAdES-XL
- XAdES-A

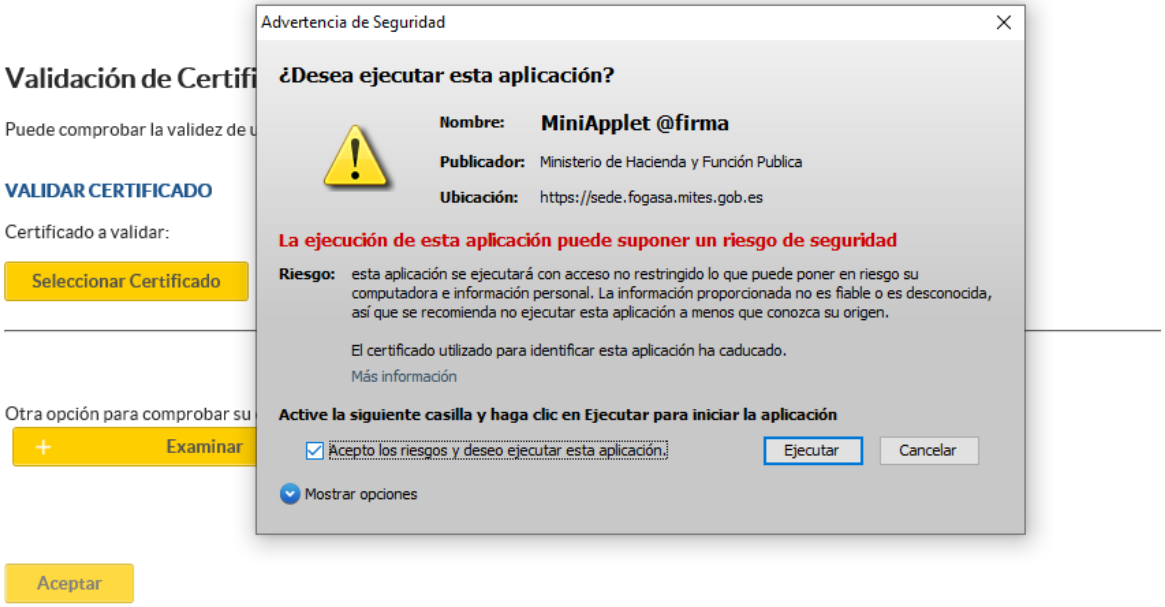
El método de firmado soportado por la plataforma es XAdES detached.

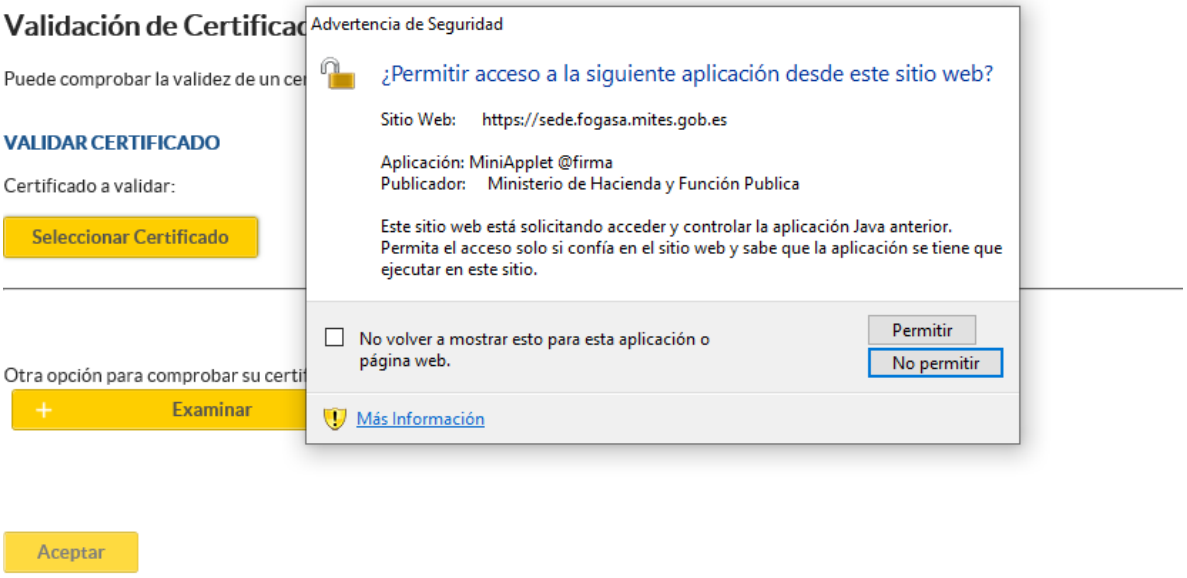
Alguno de los siguientes navegadores web con Java Runtime Environment (JRE 5 o superior) y Javascript habilitado, compatibles con el estándar HTML 4.01 del W3C

- Internet Explorer 6 o superior

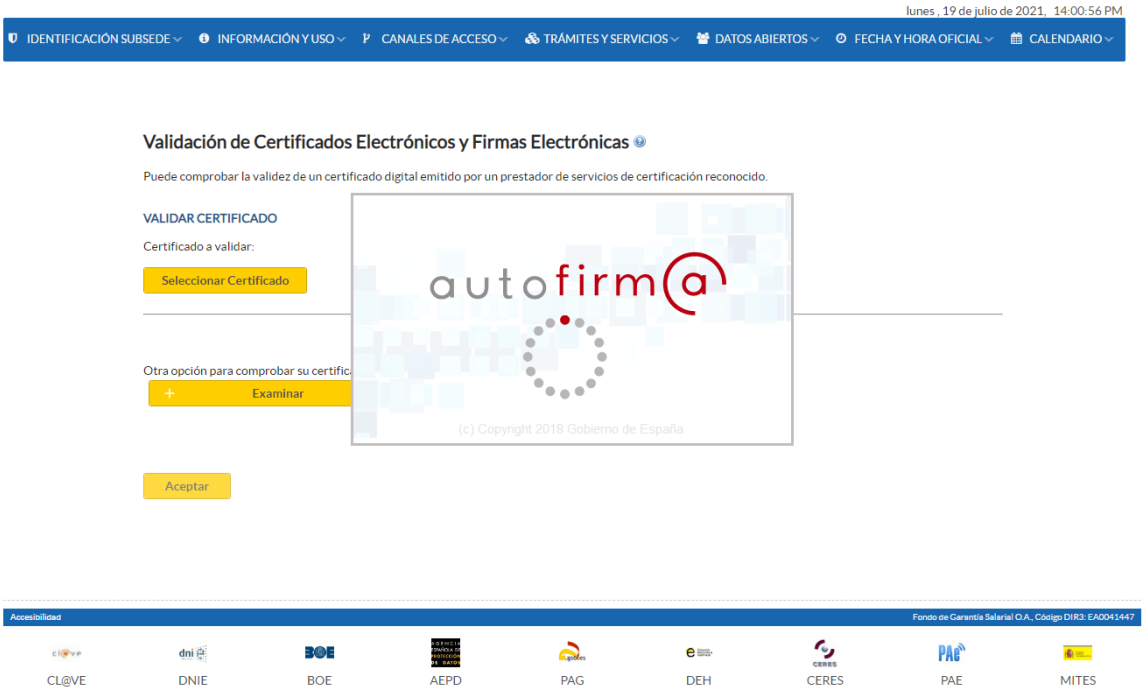
En cuanto se detecta la JVM de JAVA, se activará la llamada al **Miniapplet de @firma** y aparecerá la siguiente pantalla para aceptar:


Mensaje de página web
Se va a instalar el applet de @firma, pulse aceptar.
Aceptar


Validación de Certifi
Puede comprobar la validez de u
VALIDAR CERTIFICADO
Certificado a validar:
Seleccionar Certificado
Otra opción para comprobar su
Examinar
Aceptar
Advertencia de Seguridad
¿Desea ejecutar esta aplicación?
Nombre: MiniApplet @firma
Publicador: Ministerio de Hacienda y Función Publica
Ubicación: https://sede.fogasa.mites.gob.es
La ejecución de esta aplicación puede suponer un riesgo de seguridad
Riesgo: esta aplicación se ejecutará con acceso no restringido lo que puede poner en riesgo su computadora e información personal. La información proporcionada no es fiable o es desconocida, así que se recomienda no ejecutar esta aplicación a menos que conozca su origen.
El certificado utilizado para identificar esta aplicación ha caducado.
Más información
Active la siguiente casilla y haga clic en Ejecutar para iniciar la aplicación
Acepto los riesgos y deseo ejecutar esta aplicación.
Ejecutar
Cancelar
Mostrar opciones


Validación de Certificac
Puede comprobar la validez de un ce
VALIDAR CERTIFICADO
Certificado a validar:
Seleccionar Certificado
Otra opción para comprobar su certi
Examinar
Aceptar
Advertencia de Seguridad
¿Permitir acceso a la siguiente aplicación desde este sitio web?
Sitio Web: https://sede.fogasa.mites.gob.es
Aplicación: MiniApplet @firma
Publicador: Ministerio de Hacienda y Función Publica
Este sitio web está solicitando acceder y controlar la aplicación Java anterior. Permita el acceso solo si confía en el sitio web y sabe que la aplicación se tiene que ejecutar en este sitio.
No volver a mostrar esto para esta aplicación o página web.
Permitir
No permitir
Más Información

Para navegadores JMV, como CHROME y Mozilla Firefox 1.0 o superior con JSS, se ejecuta AUTOFIRMA.



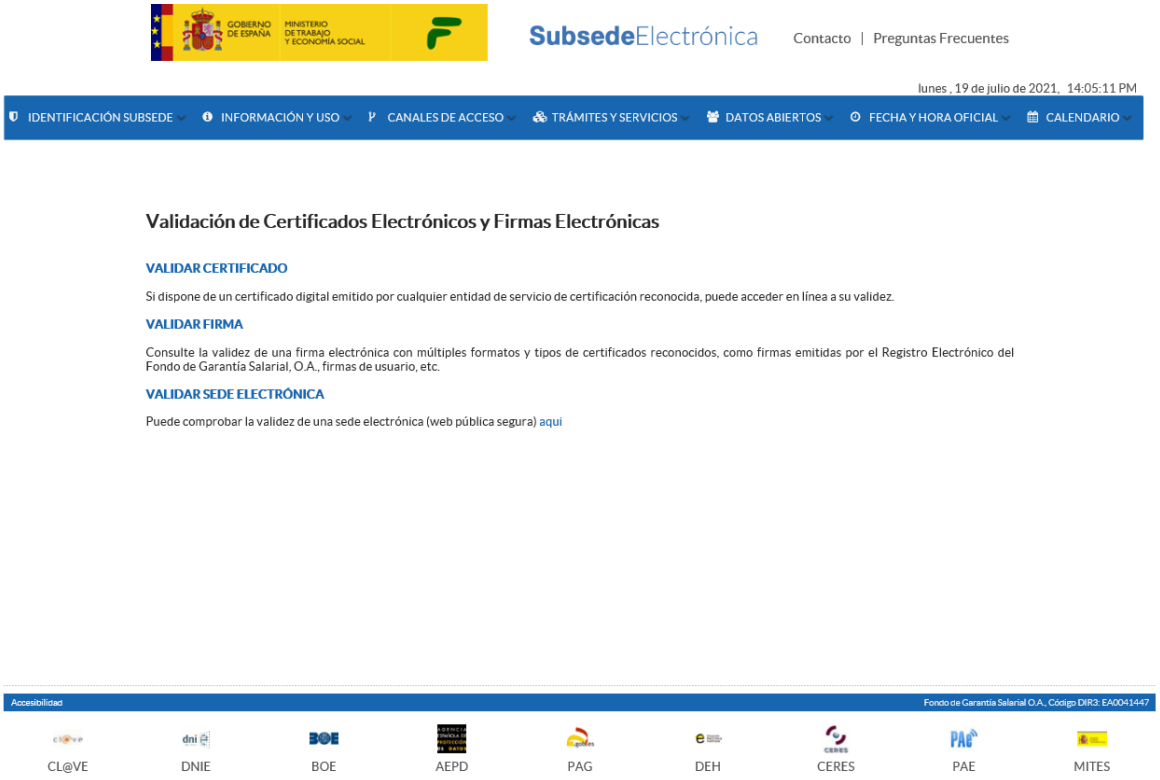
2 OPERATIVA WEB DEL SISTEMA

En este apartado se describe la parte de la aplicación del Sistema de Validación de Certificados y Firmas Electrónicas.

Dentro del conjunto de servicios actualmente existen tres procedimientos:

- Validar Certificado.
- Validar Firma.
- Validar Sede Electrónica.

2.1 IMPLEMENTACIÓN DEL INTERFAZ WEB



2.1.1 VALIDAR CERTIFICADO

Un certificado digital contiene la clave pública de un firmante, que sirve para poder verificar que una firma digital ha sido realizada con la clave privada correspondiente a la clave pública del certificado.

Un certificado digital es emitido por una Autoridad de Certificación (CA) que garantiza la relación unívoca certificado--persona.

En un certificado digital se incluyen, entre otros, los siguientes datos:

1 - Identificador único o número de serie del certificado.

2 - El algoritmo de firma digital empleado.

3 - Datos identificativos de la Autoridad de Certificación.

4 - Fechas de expedición y expiración de las claves pública y privada.

5 - Clave pública del titular del certificado.

La Autoridad de Certificación firma el certificado con su clave privada, de modo que cualquier persona puede leerlo y comprobarlo utilizando la clave pública de la propia CA (certificado padre o emisor).

Al tratarse de una firma digital, se asegura que nadie puede modificarlo, excepto la CA.

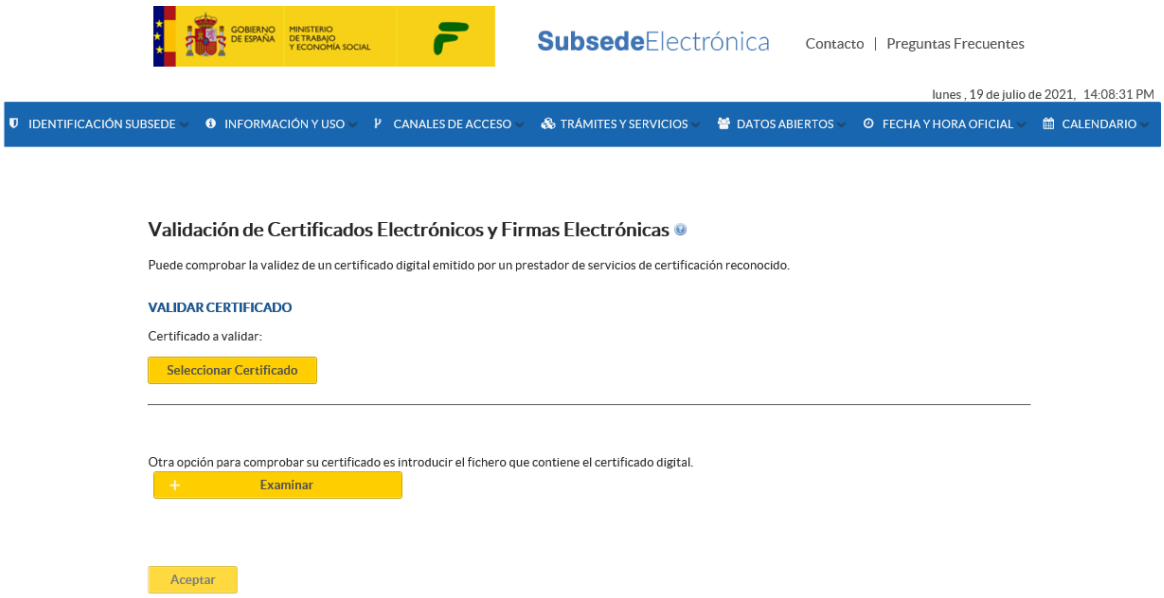
Para comprobar que un certificado pertenece a una CA de confianza, se verifica la firma digital de cada uno de los certificados que conforman la cadena de confianza (cada certificado es firmado por su padre hasta llegar al certificado raíz de la CA).

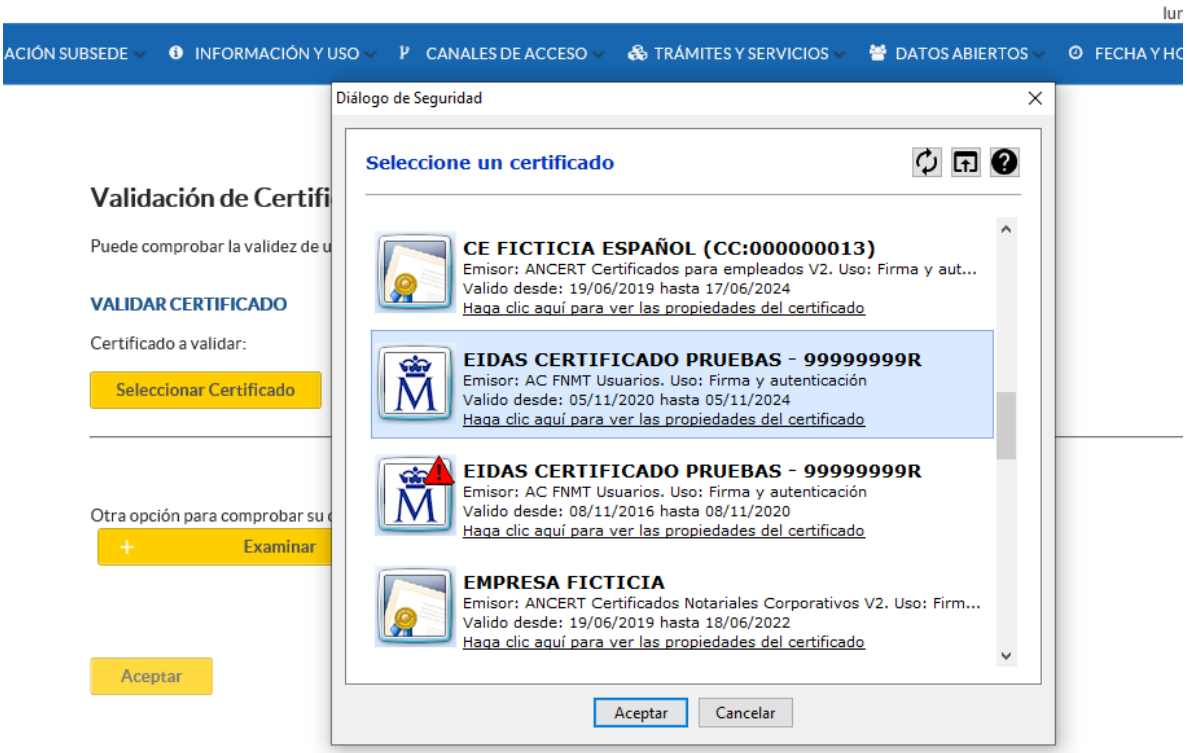
El titular de un certificado puede ser una persona física o jurídica. Además, se emiten certificados a empleados, miembros de asociaciones, empresas, colegios profesionales, ciudadanos... El uso que se le da a un certificado ha de estar recogido en la Política de Certificación y en el Contrato de emisión suscrito con la CA.

Para validar un certificado, seleccione el certificado desde la lista desplegable que muestra los certificados instalados en el navegador, o introduzca el fichero que contiene el certificado digital.

Se admiten certificados tanto en formato DER (binario) como en PEM (ASCII - base 64).

Se comprueba su integridad, periodo de validez y estado de revocación.





Validación de Certificados Electrónicos y Firmas Electrónicas

RESULTADO DE LA VALIDACIÓN

VALIDACIÓN SATISFACTORIA	✔	**Fecha de consulta:**	19/07/2021 14:11:28

Descargar Justificante

INFORMACIÓN DEL CERTIFICADO

Nombre completo:	PRUEBAS EIDAS CERTIFICADO
Dni:	99999999R
Número de serie:	968916220004456955543541057860267007 12
Organización emisora:	FNMT-RCM
Id emisor:	CN=AC FNMT Usuarios,OU=Ceres,O=FNMT-RCM,C=ES
Fecha válida desde:	2020-11-05 jue 14:04:20 +0100
Fecha válida hasta:	2024-11-05 mar 14:04:20 +0100
Tipo certificado:	FNMT PF SW EIDAS - SHA256
Id política:	MITyC
Versión política:	23
Política:	1.3.6.1.4.1.5734.3.10.1,0.4.0.194112.1.0
Clasificación:	Persona Física

Volver

2.1.2 VALIDAR FIRMA

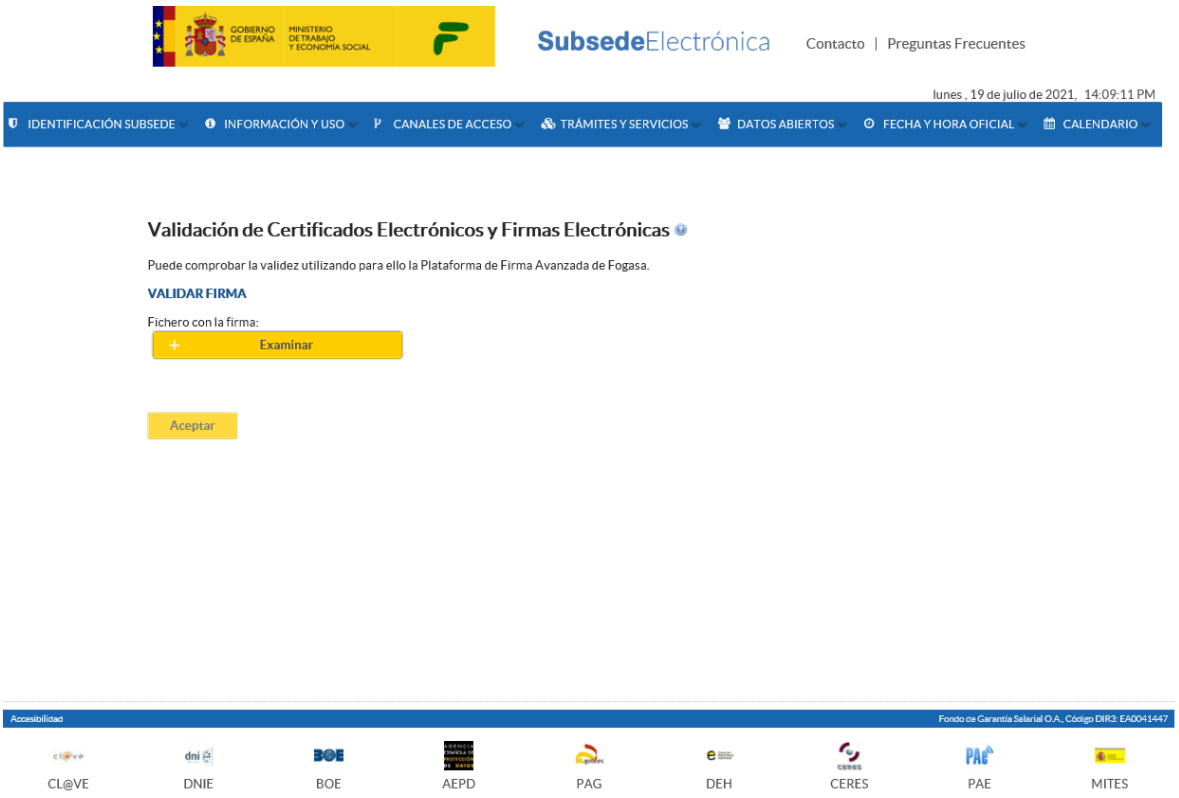
Con esta opción tendrá la posibilidad de utilizar el servicio de Validar Firma de la Plataforma de Firma Electrónica de Fogasa.

Este servicio permite realizar una validación completa de la Firma Electrónica proporcionada.

Como validación completa se entiende:

- Validación de la firma digital contenida en la Firma Electrónica frente a los datos proporcionados.
- Validación del certificado X.509 empleado y contenido en la Firma Electrónica. Se comprueba su integridad, periodo de validez y estado de revocación. Tanto el periodo de validez como el estado de revocación del certificado se comprueban frente a la fecha actual en caso que la Firma Electrónica no posea sello de tiempo o frente al mismo en caso contrario.
- Soporte del certificado. Se comprueba que el certificado y su emisor sean reconocidos y soportados por la plataforma.

Para validar una Firma, introduzca el fichero que contiene la firma. El fichero con la firma tendrá posiblemente las extensiones "xml", "txt", "xsig", "csig" o "sig".



Validación de Certificados Electrónicos y Firmas Electrónicas

RESULTADO DE LA VALIDACIÓN

VALIDACIÓN SATISFACTORIA	✔
Formato de la firma:	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-A
Fecha de consulta:	19/07/2021 14:13:34

Descargar Justificante

INFORMACIÓN DEL CERTIFICADO

Nombre completo:	[redacted]
Dni:	
Número de serie:	[redacted]
Organización emisora:	FNMT-RCM
Id emisor:	CN=AC Administración Pública,serialNumber=Q2826004J,OU=CERES,O=FNMT-RCM,C=ES
Fecha válida desde:	2018-02-05 lun 13:18:48 +0100
Fecha válida hasta:	2021-02-05 vie 13:18:48 +0100
Tipo certificado:	FNMT APE EMPLEADO PUBLICO MEDIO HW EIDAS SHA256
Id política:	MITyC
Versión política:	23
Política:	1.3.6.1.4.1.5734.3.3.4.4.1,0.4.0.194112.1.0,2.16.724.1.3.5.7.2
Clasificación:	5

SELLO DEL TIEMPO DEL FIRMANTE

Sujeto poseedor:	serialNumber=S2833002E,CN=Sello de tiempo TS@ - @firma,OU=Secretaría General de Administración Digital,O=Secretaría de Estado de Función Pública,C=ES
Fecha del sello de tiempo validada:	04/04/2019 06:11:15

Volver

2.1.3 VALIDAR SEDE ELECTRÓNICA

Enlace con Valide para la validación de la Sede Electrónica.

Valide es la aplicación de **Validación de firma y certificados Online y Demostrador de servicios de@firma**.

Además de determinar la validez de firmas y certificados digitales, se dispone de otras utilidades de valor añadido, entre las que se encuentran la generación y validación de firmas electrónicas o la demostración de servicios web de @firma, muy útil para desarrolladores e integradores de la plataforma.