CIRCUITOFIRMAS

Plataforma ligera para la firma de documentos

Universidad de Zaragoza – Administración Electrónica

Versión documento: 2.0 (10 de Octubre de 2017)

Contenido:

A) Introducción

Circuitofirmas es una aplicación que permite la gestión de solicitudes de firma de documentos. Las solicitudes de firma proceden de otras aplicaciones de tramitación y van dirigidas a empleados de la Universidad con capacidad de firma.

Esta aplicación se encarga de recibir los documentos, ponerlos a disposición del firmante o de los firmantes que deban firmarlos y devolverlos firmados a la aplicación origen. El proceso se dará por finalizado cuando todos los firmantes haya firmado, cuando alguno de ellos haya rechazado la firma o cuando se haya sobrepasado la fecha de vigencia sin que todos los firmantes hayan firmado.

Dentro de esta aplicación no se realiza ningún tipo de tramitación de los documentos, solamente se firman electrónicamente

Además de la firma digital de documentos, Circuitofirmas prevé la posibilidad de crear flujos de vistos buenos exclusivamente o vistos buenos junto con firmas electrónicas.

B) Acceso a la aplicación

El acceso a la aplicación se hace a través de un navegador y solamente es necesario disponer de acceso a internet. Aunque puede utilizarse cualquier navegador, recomendamos el uso de Mozilla Firefox o Chrome, tanto si se accede desde un ordenador, como si se accede desde un dispositivo móvil.

La URL de acceso es **https://circuitofirmas.unizar.es**

Antes de poder acceder, el firmante ha debido ser dado de alta en la aplicación y debe contar con identidad digital de UNIZAR (NIP y Contraseña administrativa) o con un certificado electrónico de persona física, empleado publico o persona jurídica.

Las cuentas de acceso para empleados de UNIZAR se crean automáticamente cuando alguien les envía una solicitud de firma desde aplicaciones como HER@LDO o desde el propio ***Circuitofirmas***.

Las cuentas de acceso para personas externas a la Universidad de Zaragoza deben crearse de forma explicita y su uso esta restringido a procedimientos especiales.

Debe tener en cuenta que aunque el acceso a la aplicación puede hacerse mediante el uso de credenciales o mediante certificado electrónico, la firma de documentos requiere siempre el uso de certificado electrónico.

El proceso de dar un Visto Bueno no requiere el uso de certificado digital, bastando con usar credenciales.

C) Información del usuario y configuración

La aplicación necesita una mínima información obligatoria de cada uno de los firmantes para su identificación y para facilitar la gestión del sistema: datos personales (nombre y apellidos), identificador oficial (NIF, NIE o Pasaporte), identificador universitario (NIP) y dirección de correo electrónico para los avisos del sistema. Junto a esta información, el usuario puede añadir en su perfil información complementaria: teléfono de contacto, dirección, cargo o rol, etc.

La dirección de correo electrónico es especialmente importante ya que se usa para avisar al firmante cada vez que deba firmar un nuevo documento o cada vez que se haya producido un acontecimiento importante en una solicitud de firma.

El rol del firmante será el que por defecto el sistema inserta en el pie de firma, pero este rol puede cambiarse para cada documento firmado, en el momento de subirlo a custodia.

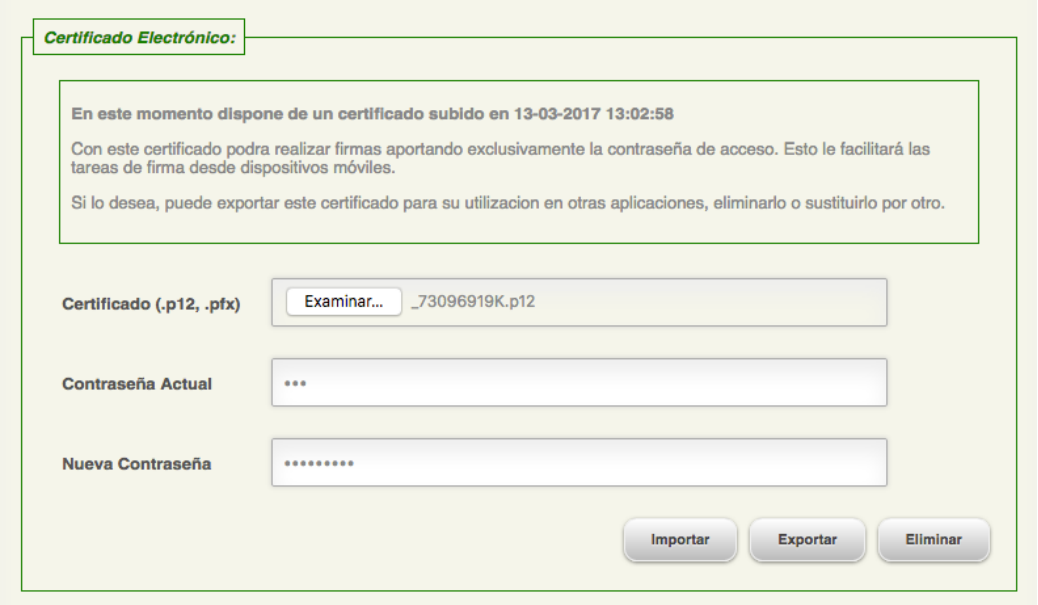
El acceso y modificación del perfil del firmante se hace desde la opción ***Configurar usuario*** del menú ***Opciones.***

En nuestro entorno, la información de los firmantes esta sincronizada con otras aplicaciones relacionadas (HER@LDO, por ejemplo) y por tanto algunos de los cambios se reflejaran en todas ellas

Cuando se reciben muchas peticiones de firma, el sistema de avisos que envía un mensaje por petición a los firmantes, puede resultar molesto. Desde la configuración de usuarios podemos establecer la política de avisos que mas nos interese.

Desde esta opción se gestiona también la importación y exportación del certificado electrónico (incluyendo la clave privada) para la firma de documentos con la opción de firma en servidor, así como el cambio de contraseña de acceso. Solamente se permite alojar en el servidor un certificado.

El certificado depositado se custodia en una base de datos especialmente securizada y auditada para evitar el uso fraudulento del mismo. El acceso a esta información esta protegido con una contraseña que solamente el propietario debe conocer.



Las opciones disponibles para la gestión de los certificados son.

Eliminar:

Permite eliminar del servidor el certificado depositado en el mismo. Sin tener un certificado en el servidor no podrá utilizar la opción de ***firma en servidor***.

Importar:

Permite subir un nuevo certificado, sustituyendo al que pueda existir en este momento.
El certificado debe proporcionarse en una archivo con formato PKCS12 que es el utilizado por la mayoría de los navegadores para la exportación/importación de certificados (normalmente se utiliza la extensión p12 o pfx).

Para poder importar el certificado debe indicar la contraseña de acceso al fichero PKCS12 (Contraseña Actual) y la contraseña con la que desea protegerlo en el servidor (Nueva Contraseña) que tendrá un mínimo de 6 caracteres.

Exportar

Permite exportar un certificado almacenado en el servidor a un fichero externo con formato PKCS12, que podrá importar en cualquier otra aplicación que lo requiera.
Deberá indicar la contraseña con la que esta almacenado en el servidor (Contraseña Actual), así como la contraseña con la que desea exportarlo (Nueva Contraseña).

Cambiar Contraseña

La contraseña de acceso al certificado es la garantía de que solamente el propietario pueda acceder a la misma y usarla. Es importante utilizar una contraseña "fuerte" y cambiarla periódicamente. Es posible que el sistema le envíe un aviso si detecta que su contraseña no es suficientemente segura. Si esto ocurre es importante que cambie su contraseña por otra mas segura,

D) Recepción y gestión de documentos para su firma. Bandejas

Una vez recibida la petición de firma, ***Circuitofirmas*** se encargará de ir avisando a cada uno de los firmantes y devolver los documentos una vez que todos los implicados han firmado. También se encarga de recordar a los firmantes que deben atender las peticiones pendientes y de devolver al tramitador aquellas peticiones que hayan caducado sin ser firmadas o que hayan sido rechazadas por alguno de los firmantes.

Desde el menú ***Acciones*** puede acceder a la lista de peticiones en las que figura como uno de los firmantes. Pulsando en la línea correspondiente a una petición accederemos a la pantalla de detalles de la misma.

El listado de peticiones puede ordenarlo por cualquiera de las columnas y el campo Buscar: le permitirá indicar un criterio de selección.

Las peticiones se muestran distribuidas en carpetas según el estado en que se encuentren. Para acceder a cada una de las carpetas use las opciones disponibles en el menú **Carpetas** o las solapas de la parte superior de la ventana.

Todas las peticiones:

Contiene una relación de todas las peticiones de firma recibidas por el firmante que no estén en situación de "archivadas". Una petición de firma pasa al estado de archivada cuando haya transcurrido 6 meses desde su recepción o cuando el usuario la haya etiquetado como tal, pulsando en el icono que aparece junto a la petición.

Peticiones Pendientes

Contiene la relación de peticiones de firma que están pendientes de ser firmadas por el usuario. Para firmarlas puede ir una a una (entrando en los detalles de cada petición) o firmarlas en bloque

seleccionándolas en el listado. En la firma en bloque no esta disponible la opción de ***firma en cliente con Autofirma***.

Peticiones En curso

Contiene la relación de peticiones de firma no finalizadas en las que el usuario es uno de los firmantes, aunque todavía no le haya llegado el turno de firma. Entrando en la pantalla de detalles podremos ver cual es el firmante que tiene el turno de firma en cada momento, los firmantes que ya han firmado y los que faltan por firmar.

Todas las solicitudes que están en estado de ***pendientes***, podremos verlas también en esta carpeta.

Peticiones Firmadas:

Incluye las solicitudes de firma que han sido firmadas correctamente por todos los firmantes. Los documentos firmados habrán sido ya devueltos a la aplicación que los creó.

Dependiendo de la aplicación origen, desde los detalles de la petición podremos acceder también a información complementaria sobre los documentos firmados (CSV, informe de firma, etc.).

Peticiones Rechazadas y/o Caducadas

Contienen la relación de solicitudes que han caducado sin ser firmadas o que han sido rechazadas por alguno de los firmantes. Los documentos incluidos ya no pueden ser firmados excepto que el tramitador vuelva a enviarlos en una nueva petición de firma.

Peticiones Archivadas

Contiene la relación de peticiones clasificadas como archivadas, independientemente de su estado. Una petición archivada podemos "desarchivarla" con lo que pasaría a su carpeta origen.

El archivado de peticiones se realiza a petición del usuario o una vez trascurrido el tiempo establecido por el firmante desde la opción Configurar Usuario. Este proceso de archivado automático se realiza una vez a la semana, por lo que una petición desarchivada puede volver a archivarse automáticamente en el siguiente ciclo.

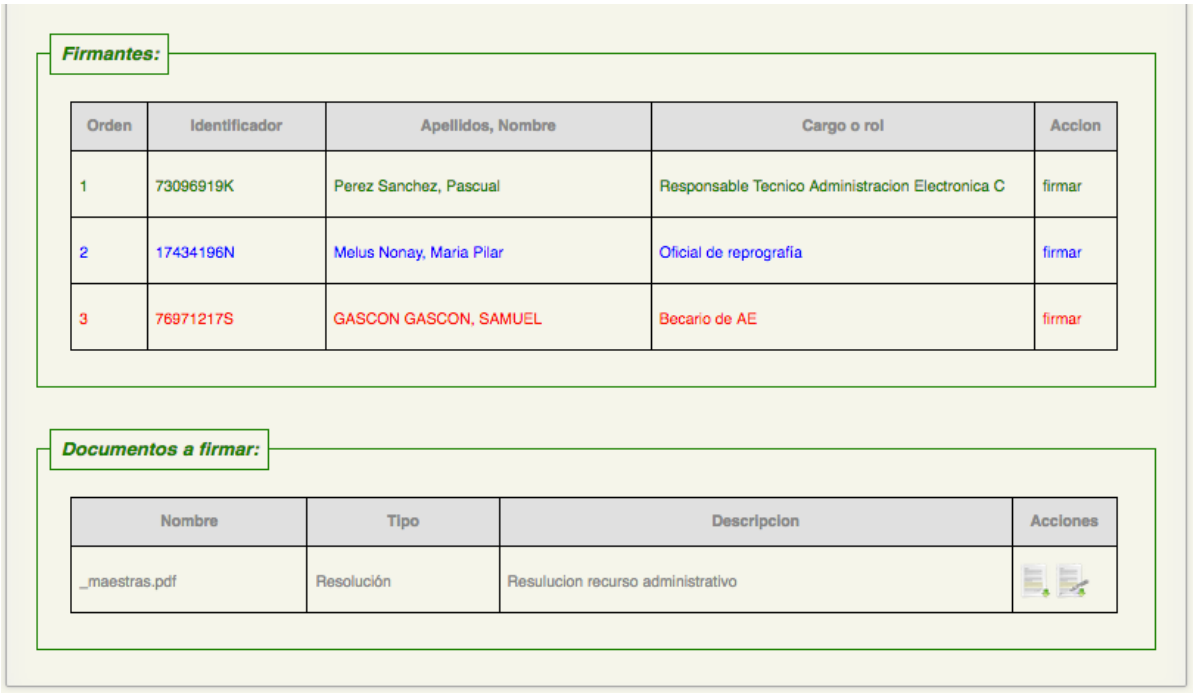
Es muy conveniente pasar a estado de archivadas aquellas peticiones que estén terminadas ya que se aligera el funcionamiento de la aplicación.

E) Proceso de firma de peticiones y métodos de firma.

Una petición solamente puede firmarse cuando esta en estado de ***pendiente***. Cuando llegue a este estado, el firmante recibirá un aviso por correo electrónico indicándole que tiene una petición en espera de firma.

Los avisos que el sistema enviará al los firmantes depende de lo que estos haya establecido en sus preferencias.

Las peticiones de firma pendiente pueden firmarse en bloque seleccionándolas desde el listado de peticiones o una a una entrando en los detalles de la misma. La firma se inicia desde el botón ***Firmar Seleccionadas*** o ***Firmar…***



Circuito de firma dispone de varios métodos de firma (todos ellos libres de los problemas derivados del uso de *applets* java) cuyo resultado es el mismo técnicamente pero que permiten a cada firmante elegir el que prefiera o el que mejor se adapte a sus circunstancias.

Firma al vuelo

La firma se realiza en un servidor de UNIZAR. No en el ordenador del usuario.

Para ello se requiere que el certificado usado para la firma, así como la contraseña de acceso a su clave privada sean enviadas al servidor de firmas. Este servidor las utilizará para firmar los documentos incluidos en la petición o peticiones a firmar y después las desechará.

En cada acción de firma deberá aportar el certificado (en un formato PKCS12) y la contraseña de acceso.

La Universidad de Zaragoza garantiza que esta información (certificado y contraseña) solamente se usan para realizar la firma y que se elimina inmediatamente al finalizar el proceso.

Firma en servidor

Este mecanismo es similar al anterior. La firma se realiza en un servidor y no en el ordenador personal del firmante.

La diferencia es que en este caso el certificado del firmante esta almacenado en una base de datos del sistema y por tanto no es necesario aportarlo cada vez que vamos a firmar. Para cada firma deberemos aportar la contraseña de acceso ya que solamente la conoce el firmante.

El certificado se guarda protegido por la contraseña de acceso que solamente conoce el firmante. Es importante usar contraseñas "fuertes"

La base de datos donde se almacenan los certificados esta especialmente protegida y se hace una auditoria continua sobre los accesos al certificado que se enviará periódicamente al firmante para su comprobación.

Es un método muy cómodo para ser utilizado desde cualquier dispositivo móvil o desde cualquier sitio con pocos recursos ya que no se requiere disponer del certificado y es compatible con cualquier navegador o cualquier dispositivo móvil.

Firma en cliente con AUTOFIRMA

Este método es el mas parecido a la firma electrónica tradicional usando *applets* java, pero sin necesidad de ellos.

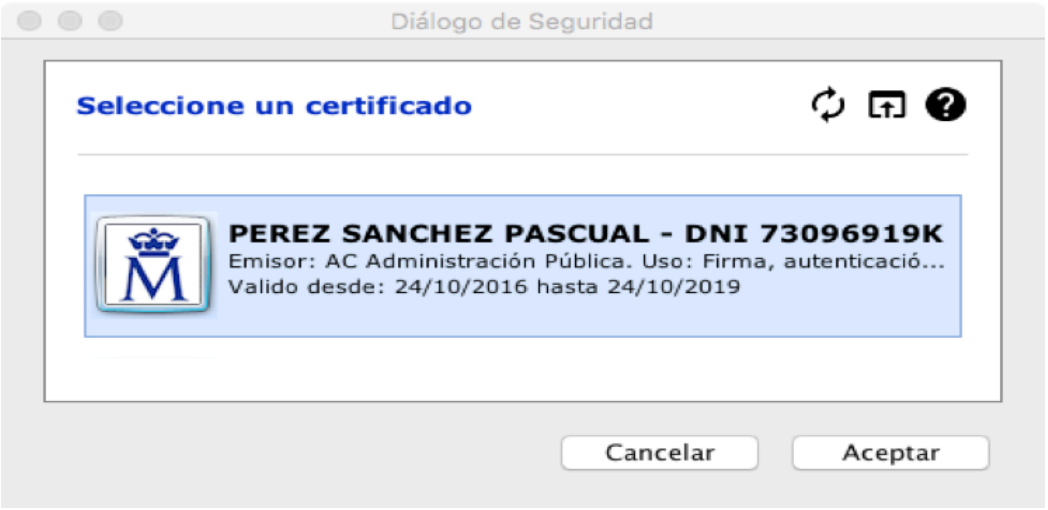
La firma se hace en el ordenador personal del firmante, no en el servidor. Por ello, ni el certificado ni la contraseña de acceso a la clave privada deben salir del ordenador del firmante.

Para que la firma pueda hacerse en el ordenador cliente, los documentos deben descargarse desde el servidor y las firmas deben enviarse al finalizar el procesos. Esto se hace de forma trasparente para el firmante, pero hace el proceso de firma mas lento (dependiendo del ancho de banda de nuestra conexión) y obliga a limitar el número de documentos a firmar cada vez.

Antes de poder utilizar usar la ***firma en cliente*** debemos instalar en nuestro ordenador la aplicación AUTOFIRMA. El proceso de instalación es muy sencillo y la versión adecuada pude descargarla desde:

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

El botón ***Firmar*** inicia el proceso de firma conectando con la aplicación AUTOFIRMA y permitiendo al firmante seleccionar el certificado a utilizar para la firma. Para que la aplicación funcione correctamente el almacén de certificados del sistema debe contener al menos un certificado válido. Use el navegador Chrome para ello.



Desde la pantalla de selección de certificados pude acceder también a certificados almacenados en ficheros PKCS12 o al eDNI

Firma con AUTOFIRMA desde dispositivo móvil

Si utilizamos la opción de firma en cliente desde un dispositivo móvil el proceso es similar a cuando usamos un ordenador personal pero tienen algunas características particulares.

Antes de nada debemos descargar desde el store correspondiente la aplicación equivalente a AUTOFIRMA que se llama ***Cliente de firma***.

También deberemos instalar el certificado electrónico. Pare ello basta con enviar al móvil un fichero PKCS12 incluyéndolo y hacerle un doble clic. Normalmente el dispositivo móvil le obligara a poner un control de acceso (contraseña, patrón, etc.) antes de instalar el certificado.

En los dispositivos móviles, la comunicación entre el navegador y la aplicación de firma debe hacerse a través de un servidor intermedio. Esto es trasparente para el firmante pero ralentiza el proceso de firma. Además, el sistema solicita la selección del certificado a usar para cada uno de los documentos.

Por todo esto, aconsejamos que si desea utilizar un dispositivo móvil para la firma de documentos opte por el método de ***firma en servidor***

F) Tramitación y custodia de los documentos firmados

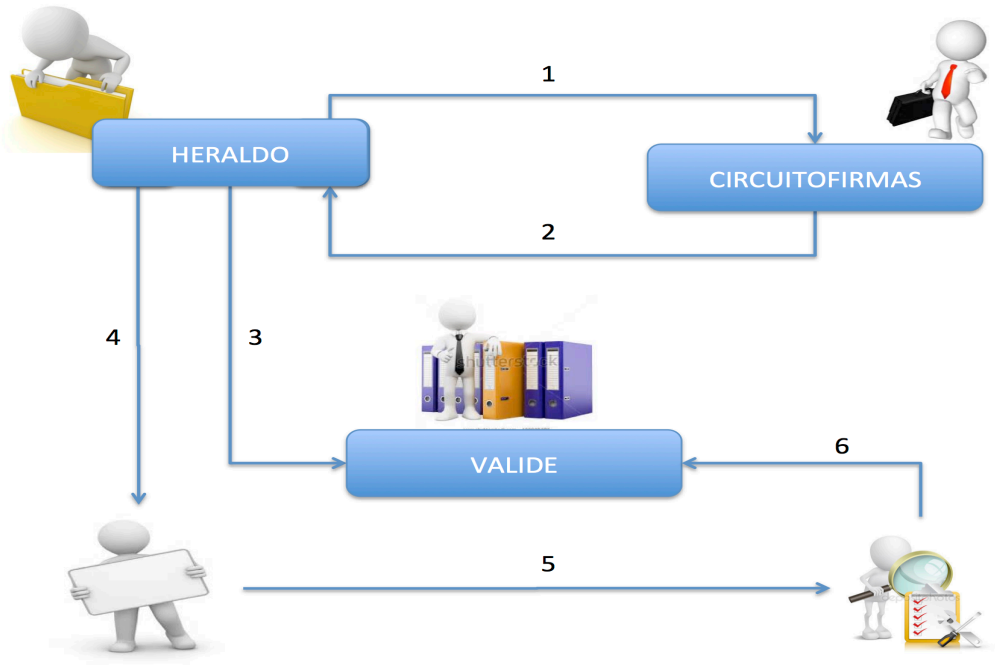
Como ya hemos comentado anteriormente, lo mas habitual es que las peticiones de firma se creen en las aplicaciones que necesitan tramitar documentos firmados, como por ejemplo HERALDO.

Estas aplicaciones y sus tramitadores son los encargadas de preparar los documentos a firmar, enviarlos a la firma y, una vez firmados, usarlos convenientemente.

Todos los documentos firmados en nombre de la Universidad de Zaragoza, una vez firmados, deben archivarse en su sistema de custodia y verificación. Para ello se les asigna un CSV (Código Seguro de Verificación), se les asignan algunos metadatos y se crea un informe de firma que pude utilizarse como copia autentica del documento original. De esta manera, cualquiera que reciba un documento firmado en UNIZAR podrá cotejarlo adecuadamente con el original.

Estas tareas son propias del tramitador más que del firmante y por ello queda fuera del alcance de la aplicación de firmas.

En el siguiente esquema podemos ver el flujo seguido por un documento desde el momento en que se prepara para su firma hasta el momento en que se presenta para que surta efectos.



1. Desde una aplicación de gestión un tramitador preparará una petición de firma consisten en uno o varios documentos y en la lista de personas que deben firmarlos. Esta petición es enviada a la aplicación ***Circuitofirma***.

2. Una vez que la petición llega a ***Circuitofirmas*** se inicia el proceso de firma avisando al primer firmante para que firme, para las firmas en CASCADA o a todos ellos para la firma en PARALELO. Los documentos irán pasando de firmante en firmante hasta que todos ellos hayan firmado. La petición, con los documentos y las firmas correspondientes vuelve a la aplicación origen y el remitente es avisado de que el proceso de firma ha finalizado.

3. Aunque los documentos firmados tienen una validez intrínseca, la política de firma de UNIZAR obliga al tramitador a subir los documentos firmados "al sistema de custodia". Este proceso asigna un CSV a cada uno de ellos y genera un informe de firma que es archivado junto con el original en el sistema de validación de la organización. Este proceso esta reservado al tramitador y el firmante no puede hacerlo de forma autónoma.

4. Una vez firmados y custodiados, los documentos puede tramitarse. Si, por ejemplo, se trata de una comunicación, podemos hacer llegar al interesado el informe de firma (o la firma original) mediante un correo electrónico.

5. El interesado receptor del documento firmado seguramente lo presentará en otra administración o ante un tercero para que surta los efectos deseados.

6. El receptor del documento firmado, debe validar la firma incorporada en el mismo. Si se esta trabajando con el informe de firma, obligatoriamente deberá realizar esta validación accediendo a nuestra sede electrónica para cotejar la copia recibida con el original custodiado. Para ello se utilizará el CSV asignado al documento e incluido en el informe de firma.

G) Crear nueva petición de firma desde *Circuitofirmas*

Aunque lo más habitual es que el proceso de firma de documentos se inicie en una aplicación de tramitación (HERALDO, por ejemplo), puede haber circunstancias concretas en las que interese que sea el firmante quien prepare un documento e inicie el proceso de firma. Un ejemplo sería la emisión de informes donde el redactor y el firmante son la misma persona.

Esta posibilidad esta disponible desde la opción "Crear nueva petición de firma" del menú Acciones y esta reservada solamente a algunos firmantes con el perfil adecuado.

Cuando se inicia la firma de documentos desde Circuitofirmas el proceso de firma es equivalente a cuando el inicio del proceso se hace desde una aplicación de tramitación, pero los documentos firmados no podrán ser enviados al sistema de custodia ni se les creara un informe de firma de forma automática, ya que estas funciones están reservadas a los tramitadores de la institución.

Por ello, si un firmante crea una nueva petición de firma desde dentro de Circuitofirmas y desea que los documentos firmados pasen al sistema de custodia de la Universidad, debe enviar la petición una vez finalizada a un tramitador para su validación y subida a custodia. Para ello se utilizara el botón "Envío a HERALDO" que aparece en los detalles de la petición de firma finalizada.

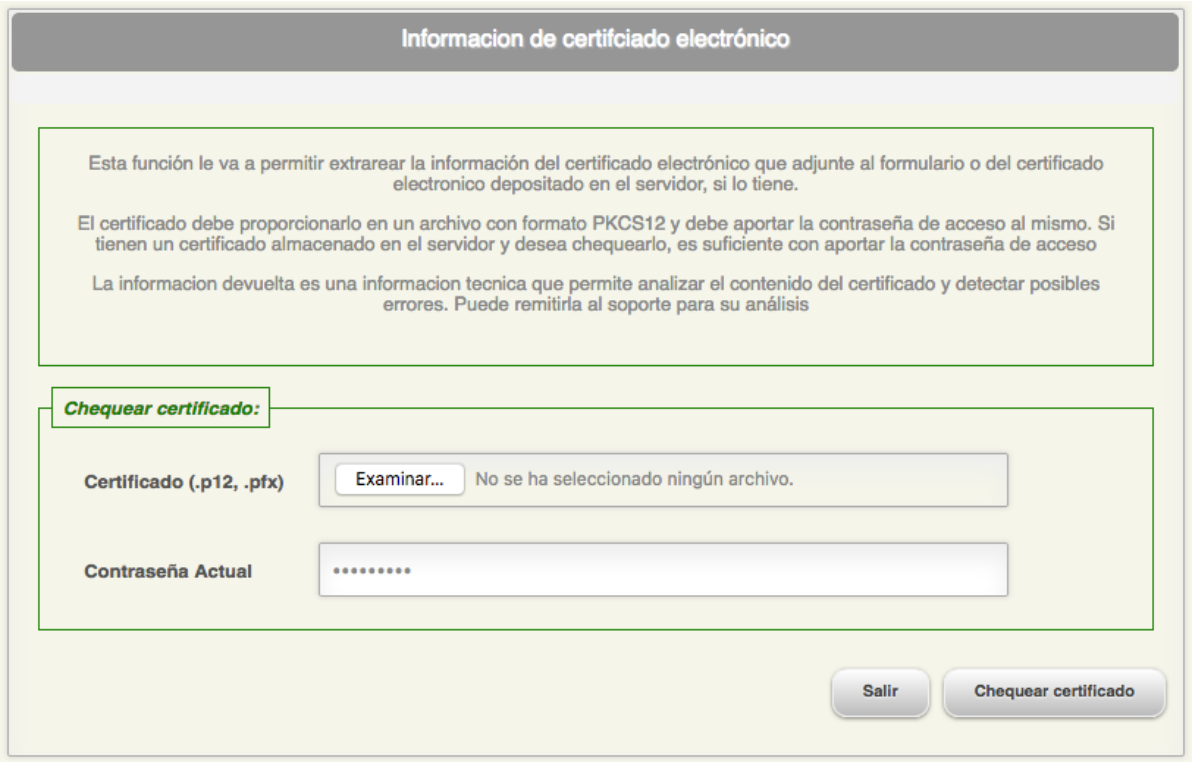
Una vez que el tramitador correspondiente haya subido los documentos al sistema de custodia, el firmante tendrá acceso al informe de firma, de la misma manera que cuando el proceso se inició en la aplicación de tramitación.

H) Validación de certificados electrónicos

Los certificados soportados por el sistema son aquellos admitidos por el Ministerio de Industria, Energía y Turismo. Se pueden consultar los certificados admitidos revisando el documento Certificados admitidos por la plataforma @firma.

Como existe una gran variedad de certificados puede ocurrir que alguno de ellos ocasione problemas al usarlo en procesos de firma, incluso aunque nos haya servido para autenticarnos. También puede ocurrir que estemos intentando usar un certificado caducado o revocado.

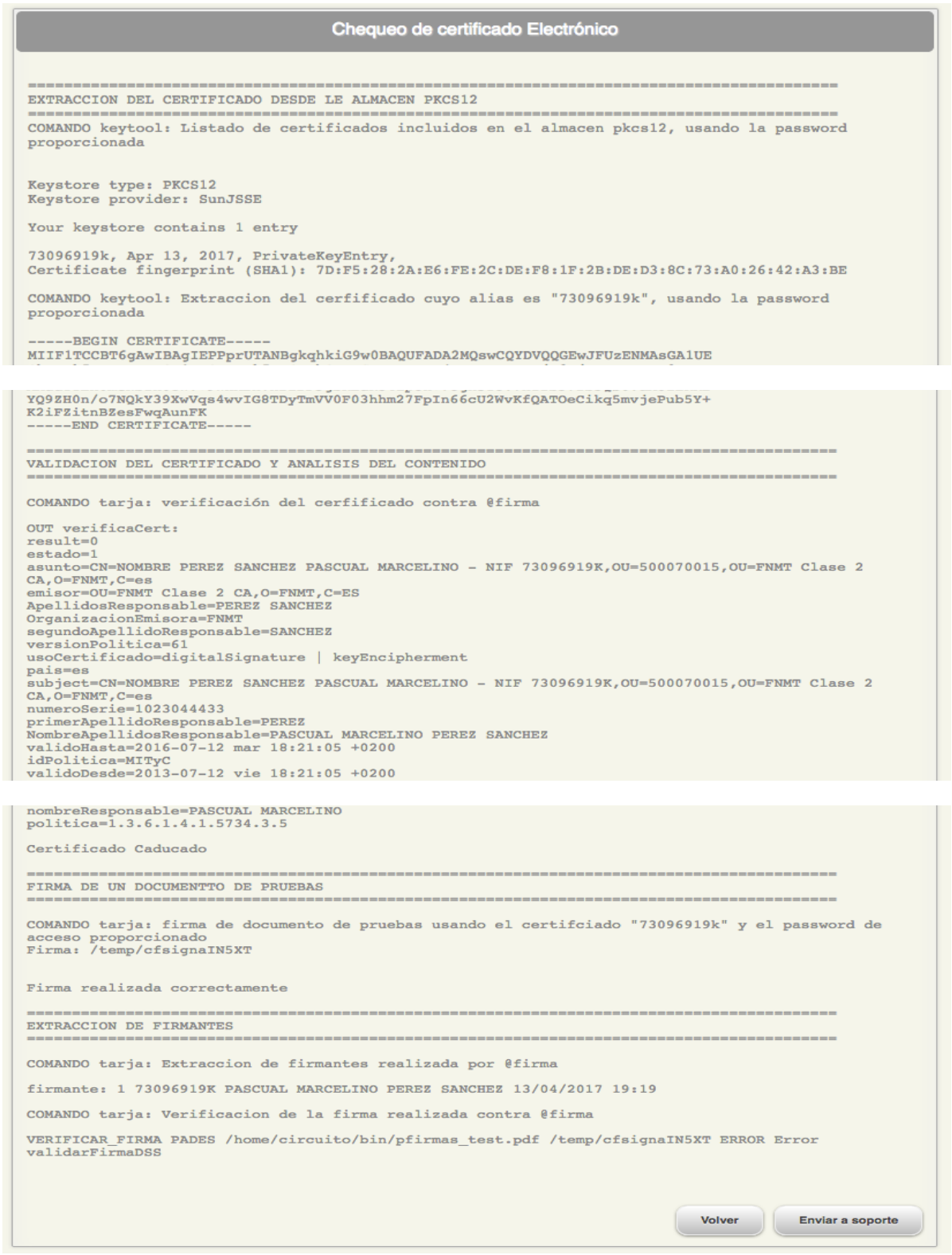
Mediante la opción ***Comprobar certificado*** del menú ***Opciones*** podremos hacer un chequeo de bajo nivel de nuestro certificado.



Para iniciar la comprobación bastará con aportar el certificado almacenado en un formato pkcs12 y la contraseña de acceso.

El proceso de verificación ejecutará una serie de acciones que van desde la extracción del certificado de su almacén, hasta la firma de un documento de pruebas. El resultado se mostrará en una pantalla similar a la del ejemplo incluido aquí.

Si tiene problemas para interpretar la información mostrada puede enviarla en un mensaje de correo a la dirección de soporte para que la analicen y diagnostiquen el problema. Este envio se hace automáticamente mediante el botón "Envío a soporte"



Chequeo de certificado Electrónico

```
==========================================================================================
EXTRACCION DEL CERTIFICADO DESDE LE ALMACEN PKCS12
==========================================================================================
COMANDO keytool: Listado de certificados incluidos en el almacen pkcs12, usando la password
proporcionada


Keystore type: PKCS12
Keystore provider: SunJSSE

Your keystore contains 1 entry

73096919k, Apr 13, 2017, PrivateKeyEntry,
Certificate fingerprint (SHA1): 7D:F5:28:2A:E6:FE:2C:DE:F8:1F:2B:DE:D3:8C:73:A0:26:42:A3:BE

COMANDO keytool: Extraccion del cerfificado cuyo alias es "73096919k", usando la password
proporcionada

-----BEGIN CERTIFICATE-----
MIIF1TCCBT6gAwIBAgIEPPprUTANBgkqhkiG9w0BAQUFADA2MQswCQYDVQQGEwJFUzENMAsGA1UE
YQ9ZH0n/o7NQkY39XwVqs4wvIG8TDyTmVV0F03hhm27FpIn66cU2WvKfQATOeCikq5mvjePub5Y+
K2iFZitnBZesFwqAunFK
-----END CERTIFICATE-----

==========================================================================================
VALIDACION DEL CERTIFICADO Y ANALISIS DEL CONTENIDO
==========================================================================================

COMANDO tarja: verificación del cerfificado contra @firma

OUT verificaCert:
result=0
estado=1
asunto=CN=NOMBRE PEREZ SANCHEZ PASCUAL MARCELINO - NIF 73096919K,OU=500070015,OU=FNMT Clase 2
CA,O=FNMT,C=es
emisor=OU=FNMT Clase 2 CA,O=FNMT,C=ES
ApellidosResponsable=PEREZ SANCHEZ
OrganizacionEmisora=FNMT
segundoApellidoResponsable=SANCHEZ
versionPolitica=61
usoCertificado=digitalSignature | keyEncipherment
pais=es
subject=CN=NOMBRE PEREZ SANCHEZ PASCUAL MARCELINO - NIF 73096919K,OU=500070015,OU=FNMT Clase 2
CA,O=FNMT,C=es
numeroSerie=1023044433
primerApellidoResponsable=PEREZ
NombreApellidosResponsable=PASCUAL MARCELINO PEREZ SANCHEZ
validoHasta=2016-07-12 mar 18:21:05 +0200
idPolitica=MITyC
validoDesde=2013-07-12 vie 18:21:05 +0200
nombreResponsable=PASCUAL MARCELINO
politica=1.3.6.1.4.1.5734.3.5

Certificado Caducado

==========================================================================================
FIRMA DE UN DOCUMENTTO DE PRUEBAS
==========================================================================================

COMANDO tarja: firma de documento de pruebas usando el certifciado "73096919k" y el password de
acceso proporcionado
Firma: /temp/cfsignaIN5XT


Firma realizada correctamente

==========================================================================================
EXTRACCION DE FIRMANTES
==========================================================================================

COMANDO tarja: Extraccion de firmantes realizada por @firma

firmante: 1 73096919K PASCUAL MARCELINO PEREZ SANCHEZ 13/04/2017 19:19

COMANDO tarja: Verificacion de la firma realizada contra @firma

VERIFICAR_FIRMA PADES /home/circuito/bin/pfirmas_test.pdf /temp/cfsignaIN5XT ERROR Error
validarFirmaDSS
```

Volver | Enviar a soporte

I) Validación de documento firmado electrónicos

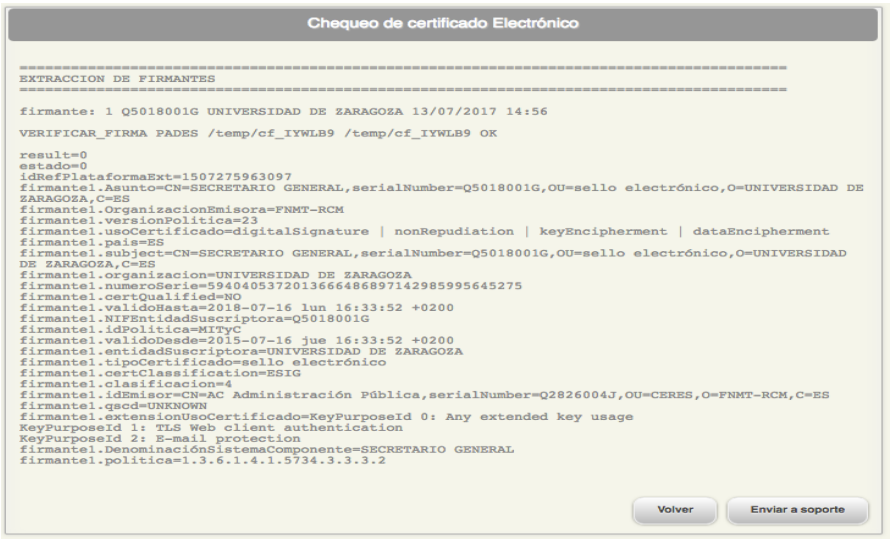
Una de las problemáticas mas comunes ligadas al uso de firma digital es la verificación de los documentos firmados: ¿este es un documento firmado? ¿Quién lo ha firmado? ¿con que certificado?...

La respuesta a estas preguntas no siempre es trivial ya que existen varios formatos de firma y su verificación no es automática.

Por otra parte, estamos habituados a manejar como sustitución del documento firmado lo que conocemos como "informe de firma" o "copia autentica de documento firmado", que es una representación en formato PDF del documento original, junto con la información relativa a los firmantes y al sistema de verificación. Sin embargo, este documento NO ES el original firmado, aunque jurídicamente ES EQUIVALENTE.

La verificación de un "informe de firma" debe hacerse en la sede electrónica del organismo que lo emitió mediante el uso del CSV y realizando un cotejo visual de la copia que nos entregan con la copia "custodiada" por el emisor. No existe un modo automático de verificación.

Si queremos verificar el original de un documento firmado electrónicamente debemos apoyarnos en algún servicio de verificación. A nivel nacional podemos hacerlo usando los servicios existente en https://valide.redsara.es o desde la opción "Comprobar firma" del menú opciones de Circuitofirmas. Ambos sistemas realizan las mismas comprobaciones: comprobar que el documento esta firmado, verificar que la firma es correcta, verificar que no se ha modificado el originar tras la firma, verificar que el certificado con que se firmo el documento es correcto y esta en vigor.



J) Uso de certificados electrónicos en Circuitofirmas

Circuito firmas es una plataforma de firma electrónica de documentos y por tanto necesita para su utilización tener acceso al certificado electrónico del firmante. Para facilitar las tareas de firma hacemos un uso de los certificados algo diferente al de otras herramientas de firma que es conveniente aclarar

a. ***Acceso a la aplicación***

   El acceso a Circuitofirmas podemos hacerlo utilizando credenciales (NIP y Contraseña) o utilizando certificado electrónico (o eDNI). Para poder acceder con certificado debemos tener "instalado en el navegador" nuestro certificado digital o tener conectado un dispositivo que permita al navegador acceder al eDNI.

   Podemos acceder al sistema usando claves o utilizando un certificado, pero utilizar otro en las operaciones de firma.

b. ***Firma al vuelo***

   Para poder firmar con este método necesitamos tener el certificado exportado en un fichero externo al navegador. No podremos usar directamente el certificado que tenemos configurado en el navegador, pero podremos exportarlo para su utilización en la firma.

   Si tiene problemas para exportar el certificado consulte la documentación.

c. ***Firma en servidor***

   Como en el caso anterior, para firmar en servidor no es suficiente con tener el certificado instalado en el navegador. Necesitamos instalar nuestro certificado de firma en el servidor. Para ello debemos utilizar la opción "Configurar usuario" del menú Configuración.

   Antes de poder subir el certificado al servidor, deberemos exportarlo desde el navegador si es que no lo tenemos ya.

d. Firma con autofirma

   Al contrario que en los anteriores, este método de firma se apoya en los certificados accesibles desde el navegador (los que tenemos instalados o el eDNI).

   Solamente podremos usar este método si estamos invocándolo desde el navegador donde tenemos el certificado:

e. ***Realización de Vistos Buenos***

   Para hacer un visto bueno de un documento no se utiliza el certificado y por tanto no necesitamos tenerlo.