Firma Electrónica en UNIZAR

Semana de Administración Abierta
Teruel, 9 de Mayo de 2018

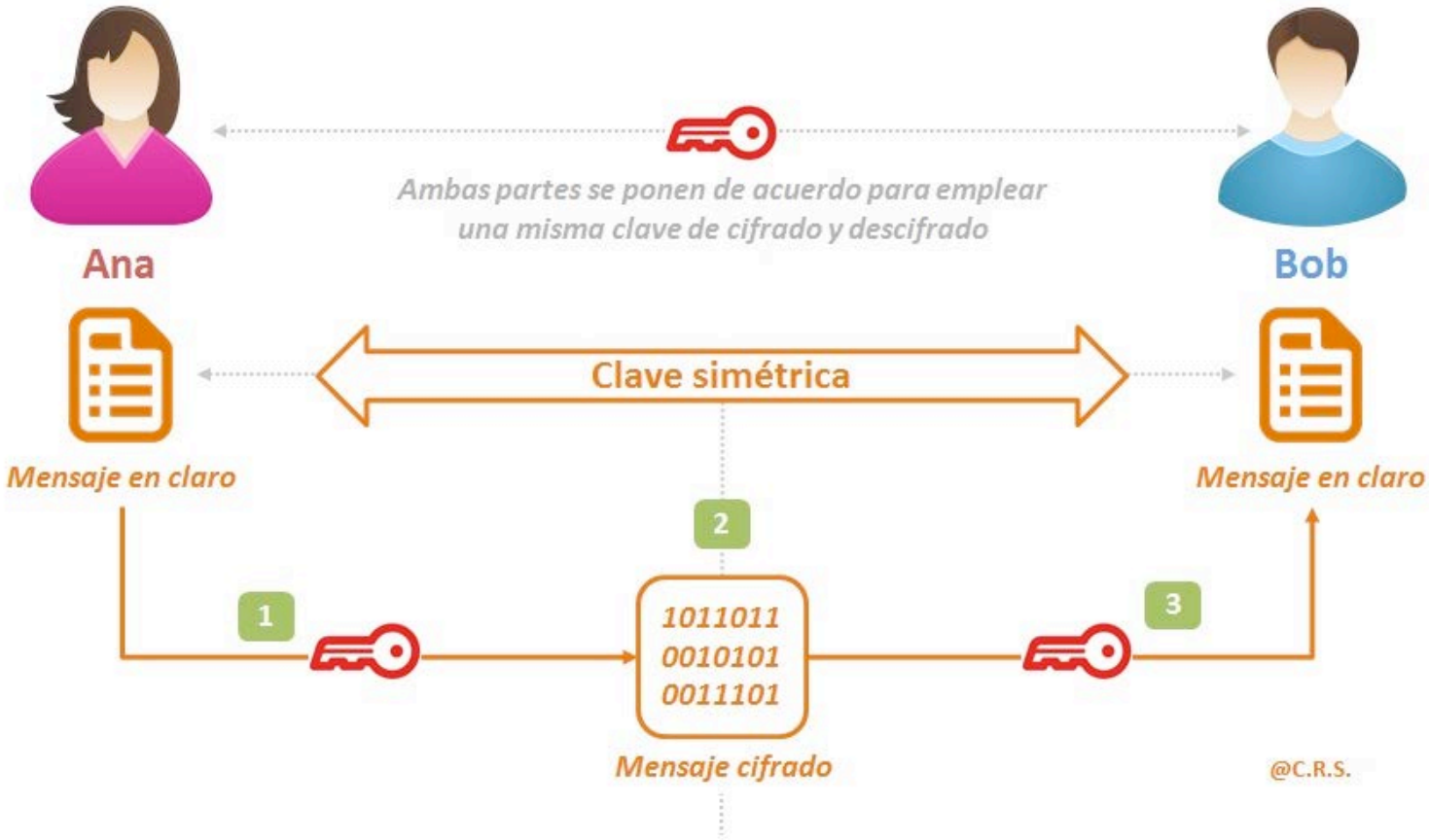
Pascual Pérez Sánchez
pascual.perez@unizar.es

Campus Universitario de Teruel
Salón de Actos del Vicerrectorado

guión

1. **Certificados electrónicos**
   - Claves simétricas y asimétricas
   - ¿Qué son los certificados electrónicos?
   - ¿Como solicitarlos?
   - ¿Donde guardarlos?
2. **¿Qué es la firma electrónica?**
   - ¿Qué pretende garantizar la firma electrónica?
   - La función hash
   - Proceso de firma y verificación.
   - Firma original e informe de firma
3. **Aplicaciones de firma**
   - La firma en escritorio
   - La firma en aplicaciones web
   - Modos de firma
4. **La firma en la Universidad de Zaragoza**
   - Solicitud de certificado de empleado público
   - Integración de las herramientas de firma: HER@LDO y CIRCUITOFIRMAS
   - Esquema de la firma de actas
   - Custodia y verificación de documentos firmados por UNIZAR

Clave simétrica

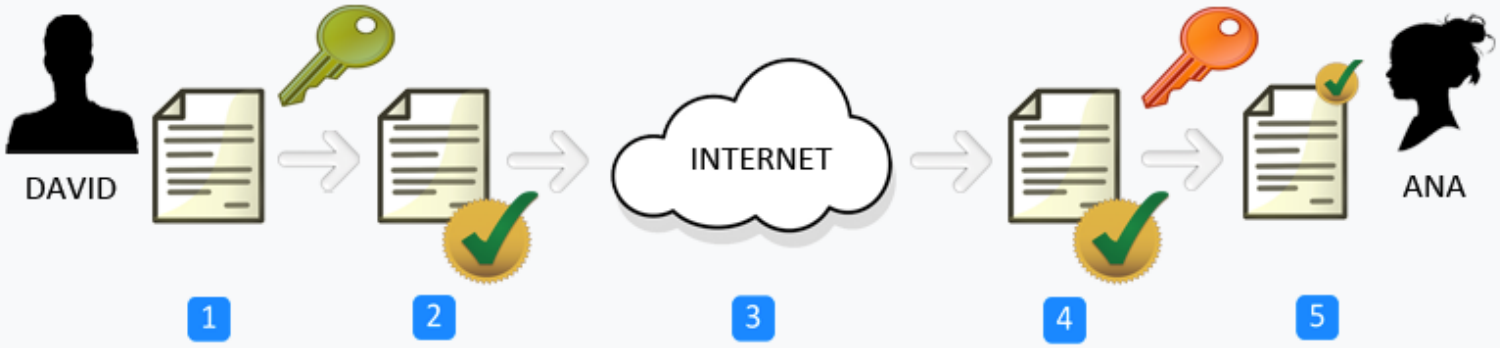


Necesitamos un medio para compartir la clave lo que implica conocer a la otra persona y confiar en el canal de comunicación.

Esto lo hace inviable para su uso generalizado en internet

Clave asimétrica

Ejemplo de firma digital con clave asimétrica: *David envía un mensaje a Ana*



1. David redacta un mensaje.
2. David firma digitalmente el mensaje con su **clave privada**.
3. David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
4. Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la **clave pública** de David.
5. Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente.

Necesitamos que un tercero de confianza certifique que la clave publica de una persona es realmente de esa persona y no de otra para evitar la suplantación:

Esto da lugar a la necesidad de los certificados electrónicos

Certificado electrónico

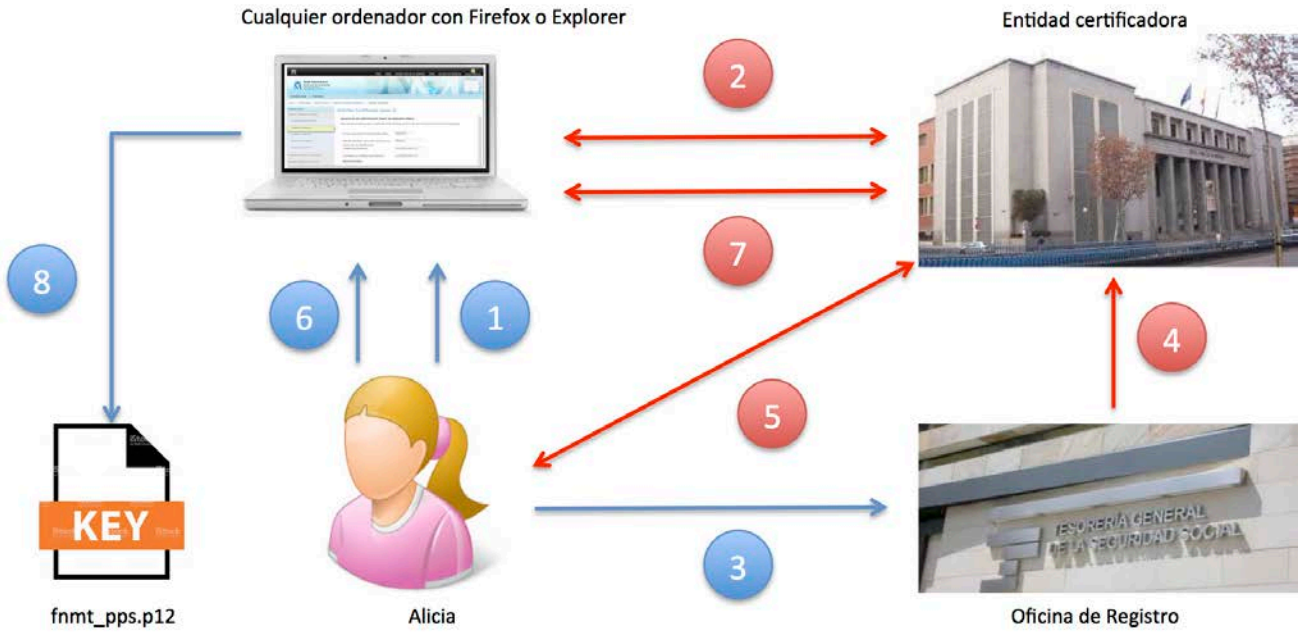
Un **certificado electrónico** es un fichero informático que contiene:

- La **clave publica** del titular
- La identidad del titular: datos personales, mail, datos de la organización, etc.
- Datos propios del certificado: número de serie, fecha de caducidad, etc.
- Información de la entidad que lo emite. P.e.: la FNMT (Fabrica Nacional de Moneda y Timbre)

Tipos de certificados

- Según el tipo de titular:
  - Certificado personal
  - Certificado de empleado publico
  - Certificado de entidad jurídica
- Según la autoridad de certificación
  - La FNMT
  - La Policía
  - Emitidos por colegios profesionales
  - Emitidos por Comunidades Autónomas

Solicitud de certificado personal



1. **Alicia entra en la web de la FNMT con un navegador y solicita un certificado personal**
2. El navegador genera un par de claves (privada y publica) y solicita la certificación de la clave pública.
   La FNMT recibe la solicitud y genera un código de solicitud que devuelve al navegador.
3. **Alicia se persona físicamente en una Autoridad de Registro (TSS, por ejemplo) con su DNI y el código de solicitud**
4. La Autoridad de Registro valida la identidad de Alicia y lo comunica a la FNMT
5. La FNMT envía un mail a Alicia indicándole que ya puede descargar el certificado
6. **Alicia solicita la descarga del certificado (usando el mismo ordenador y navegador usado para hacer la solicitud).**
7. La FNMT envía el certificado al navegador que lo deposita en el almacén de certificados.
8. **Alicia hace una copia del certificado (junto con la clave privada) para usarlo si lo desea en otro navegados o en una aplicación de firma**


Plaza Bretón
Plaza de la Bolamar
N-420a
Ctra. Villaspesa
Plaza del San Juan
Plaza del
Tor Plaza
N-420a
N-420a
DELEGACION PROVINCIAL DE TERUEL
SAN FRANCISCO, 1
DIPUTACIÓN PROVINCIAL DE TERUEL
Plaza de San Juan, 7
A.E.A.T.
PLAZA DE SAN JUAN, 3
INSS
CALLE JOAQUÍN ARNAU, 22
MINISTERIO DE ADMINISTRA-CIONES PUBLICAS
PLAZA DE SAN JUAN, 4
TGSS
PASEO GLORIETA, 1
CNMV
Personas físicas
Representante
Personas físicas y representante

Almacenes de certificados

- **Almacenes del Sistema Operativo**
  - Lo comparten “todas los navegadores” excepto Firefox.
  - Macox ->Aplicación Acceso a llaveros
  - Windows-> Navegador Explores o Chrome
- **Almacén Firefox**
  - Solamente Firefox puede acceder a ellos
  - Acceso desde Opciones->Avanzado
- **En fichero PKCS12**
  - Exportación o copia a un fichero: .p12 o .pfx
  - Puede ser usado desde Autofirma, Her@ldo y Circuitofirmas
- **eDNI**
  - Varios certificados insertados en el chip de la tarjeta
  - No pueden extraerse los certificados
  - Para acceder hay que instar los drivers adecuados
- **Almacén del servidor UNIZAR**
  - Se maneja desde HERALDO y desde Circuitofirmas. Misma base de datos
  - Uso para firma en Heraldo y Circuitofirmas
  - Usable como copia de seguridad del certificado y accesible desde cualquier sitio

Demo

- Solicitar un certificado de la FNMT
- Exportar un certificado desde Firefox
- Chequeo del certificado en Circuitofirmas

Documentación

- http //www.unizar.es: Administracion Electronica, i sombreada
- http://sededocumentacion.unizar.es/manciu/obtener_instalar_certificado.html
- http://www.cert.fnmt.es/certificados

Firma electrónica

La firma electrónica es **un conjunto de datos electrónicos** que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- ***Asegurar la integridad del documento firmado***. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación. Para ello se utiliza la **función HASH**

- ***Identificar al firmante*** de manera inequívoca. Para ello incluye el **certificado del firmant**e. Avalado por una Autoridad de Certificación reconocida

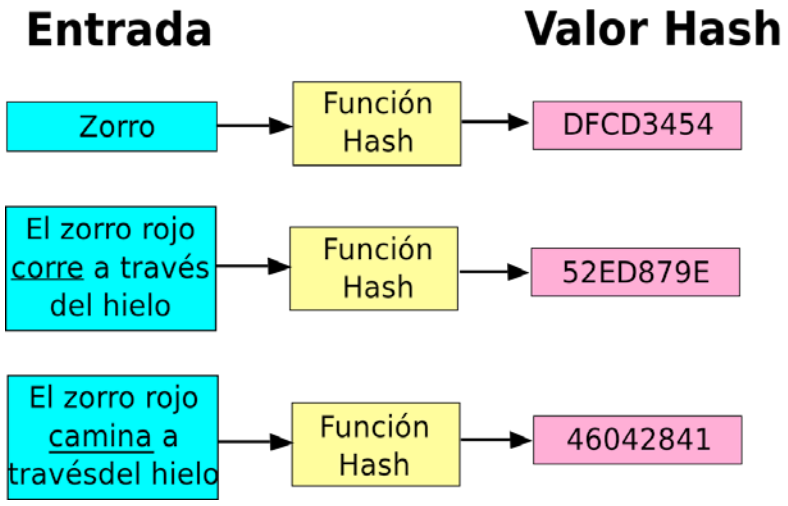
- ***Garantizar el "no repudio" en origen*.** Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos (**clave privada**) y, por tanto, posteriormente, no puede decir que no ha firmado el documento.

La base legal de la firma electrónica está recogida en la *Ley 59/2003 de Firma Electrónica* que establece en que condiciones la firma electrónica es equiparable a la firma manuscrita

La función HASH

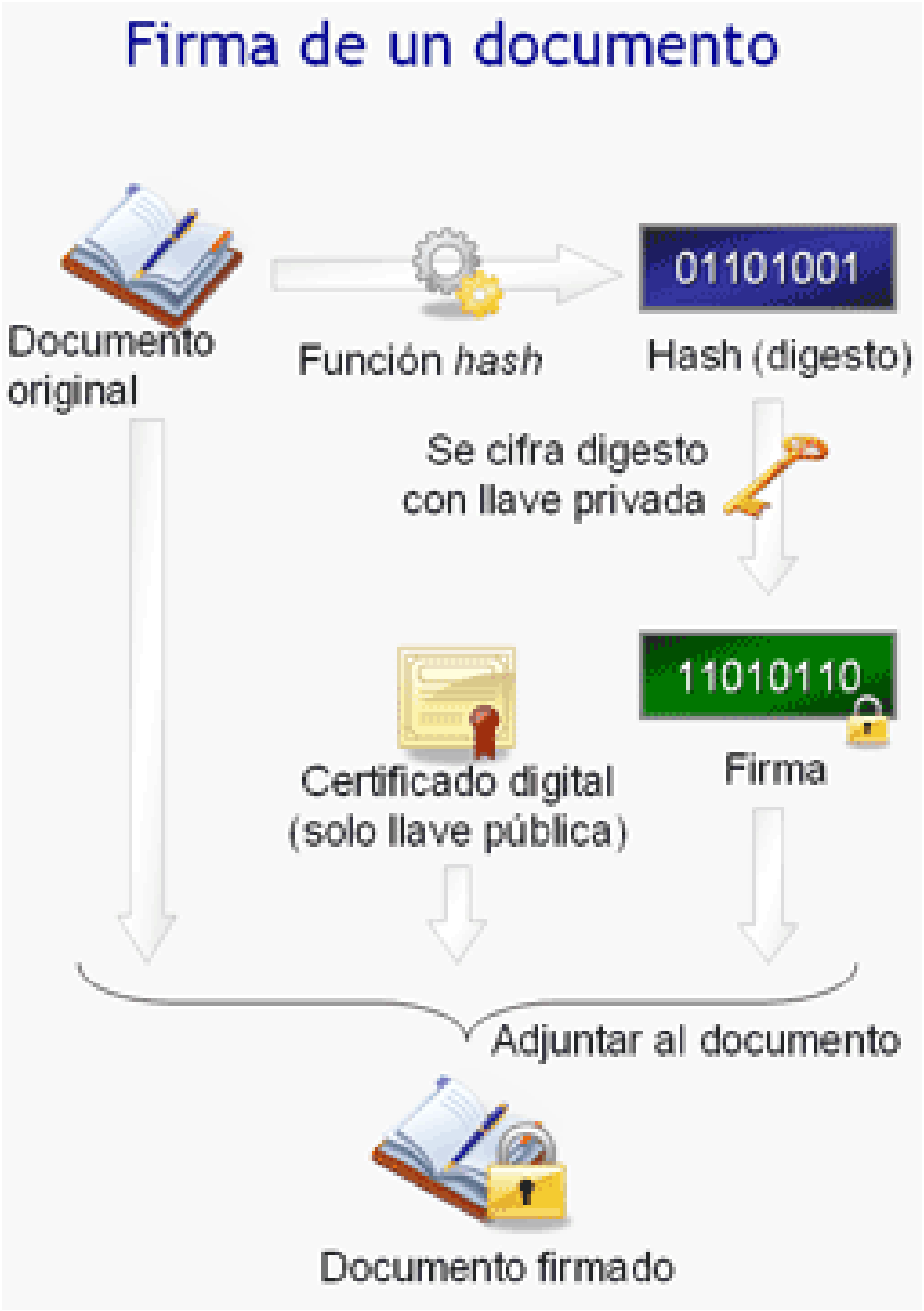
Los **hash** o "funciones de resumen" (*digest*) son algoritmos matemáticos que consiguen crear una salida alfanumérica única de longitud fija a partir de una entrada (un texto, un documento, una imagen, etc.) de longitud variable.

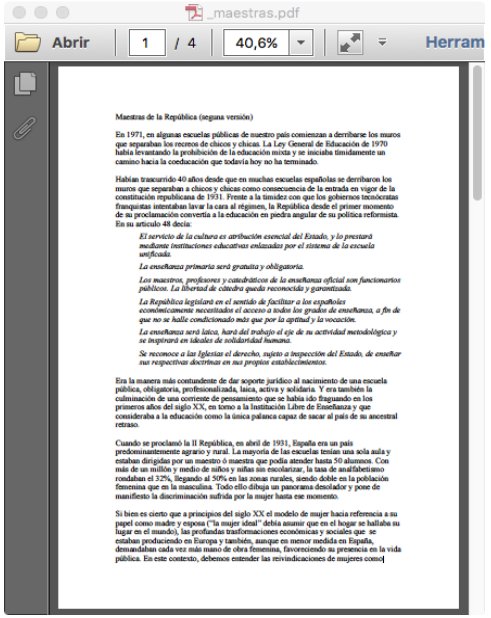
- **No son reversibles**: A partir del hash no puede componerse el texto origen
- **Son únicas**: A partir de dos entradas diferentes no puede obtenerse el mismo hash
- **Tienen una longitud fija**, independientemente del tamaño de la entrada

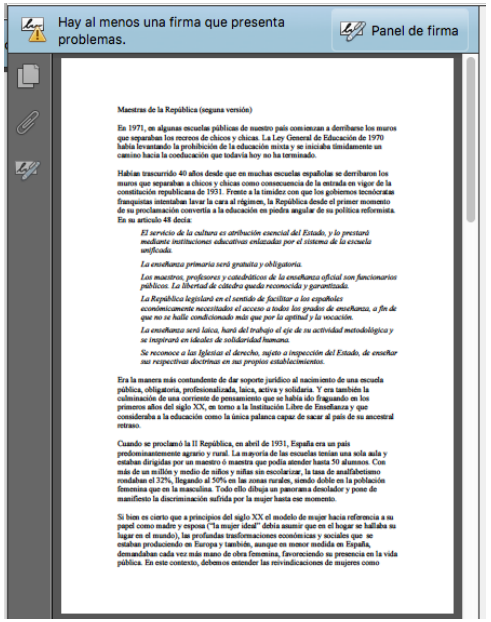


Algunas aplicaciones:

- Garantizar la integridad de un documento electrónico
- Son fundamentales en la firma electrónica
- Almacenamiento único de documentos y mensajes
- Gestión de contraseñas
- Creación *Blockchains*, base para el uso e monedas criptográficas (bitcoin, p.e.)


Firma de un documento
Documento original
Función hash
01101001
Hash (digesto)
Se cifra digesto con llave privada
11010110
Firma
Certificado digital (solo llave pública)
Adjuntar al documento
Documento firmado


_maestras.pdf
Abrir
1 / 4
40,6%
Herram
Maestras de la República (segunda versión)


Hay al menos una firma que presenta problemas.
Panel de firma
Maestras de la República (segunda versión)

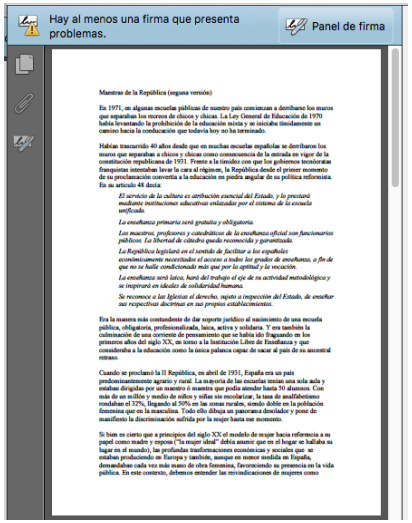
Validación de la firma

- Verificar la firma en local
- Verificar certificado en @firma

https://valide.redsara.es

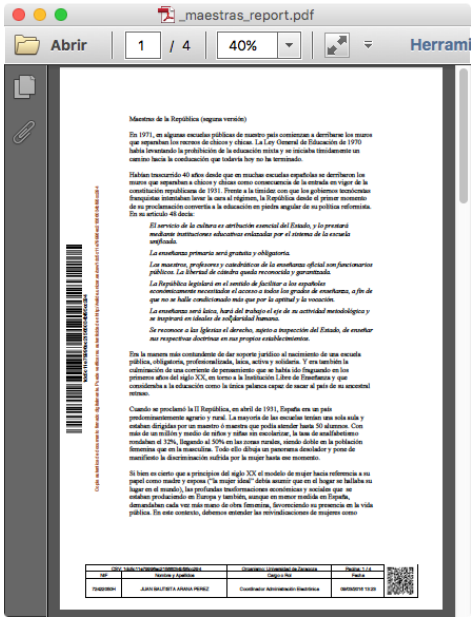
https://circuitofirmas.unizr.es

El *informe de firma*



- **Documento firmado electrónicamente**
  - Varios formatos: XADES, PADES, CADES, FACE
  - Pensado para tratamiento automático
  - Firma no visible excepto para el formato PADES
  - Solamente incluye identificación del firmante
    - NIF, nombre y apellidos
    - Certificado usado para firmar

- **Informe de firma de documento firmado**
  - Representación del documento firmado y las firmas
  - Verificable “visualmente” por cotejo
  - No es una firma pero es equivalente jurídicamente
  - Necesita un sistema de custodia para su validación
  - Contiene un Código Seguro de Verificación (CSV)
  - Requiere conversión a PDF del original. Puede causar algún problema



Aplicaciones para firmar I

- **La firma en escritorio o firma en cliente**
  - Para firmar documentos que tenemos en el ordenador o que previamente los hemos descargado.
  - La firma se hace utilizando una aplicación instalada en nuestro ordenador.
  - Existen varias. Aconsejable Autofirma con versión para MAC y para Windows
  - Permiten usar certificados en diferentes almacenes: el de S.O, en pkcs12, en eDNI
  - Permiten añadir firmas a un documento ya firmado
- **Casos de uso**
  - Si debemos firmar un documento privado
  - Añadir nuestra firma a un documento compartido ya firmado por otra persona
  - Firmar un documento elaborado por nosotros para incorporarlo después en el sistema genérico de firmas

Aplicaciones para firmar II

- **La firma desde aplicación web**

  - La firma suele ser una de las fases en un procedimiento administrativo que se encarga de preparar los documentos a firmar y del posterior tratamiento:
    - Firmar un documento para publicarlo en el Tablón de anuncios
    - Firmar una resolución que se notifica a un interesado
    - Firmar un certificado de calificaciones solicitado por un estudiantes

  - En UNIZAR un ejemplo de este tipo de aplicación es HER@LDO

  - Son típicas las aplicaciones web especializadas en la gestión de flujos de firma que simulan los "**portafirmas**" utilizados tradicionalmente:
    - Los documentos a firmar se reciben desde distintas aplicaciones de gestión
    - Los firmantes reciben todas las ordenes de firma en el momento adecuado
    - Una vez finalizada la firma, el documento firmado vuelve a la aplicación origen
    - En UNIZAR utilizamos dos aplicaciones: Portafirmas (MINHAP) y Circuitofirmas desarrollado por nosotros

Aplicaciones para firmar III

- **La firma desde aplicación web. Modos de firma**

  - Firma en cliente:
    - La aplicación web lanza una aplicación de firma en el ordenador del usuario:
      - applets java (muy problemáticos) por los problemas de seguridad que crean
      - Invocación por protocolo a una aplicación de firma de escritorio como AUTOFIRMA
    - Los documentos se descargan en el cliente y una vez firmados se envían al servidor
    - La clave privada del firmante no sale de su PC

  - Firma en servidor
    - La aplicación web ejecuta una aplicación de firma residente en el servidor.
    - Los documentos no deben viajar entre el servidor y el cliente
    - Se facilita la movilidad: movil, tableta, cualquier PC
    - La clave privada debe estar accesible al servidor, bien porque se guarda en una base de datos, bien porque se envía desde el cliente para cada firma (“firma al vuelo”)

  - Firma CL@VE
    - Es una implementación “oficial” de la firma en servidor.
    - El firmante solicita un certificado de firma que se guarda en un servidor de la Seguridad Social
    - El sistema esta todavía en una fase incipiente de implantación.

Demos

- Generación de hash:
  http://www.convertstring.com/es/Hash/SHA256
- Firmar con AUTOFIRMA
- Firmar con Circuitofirma
- Verificar una firma y un certificado

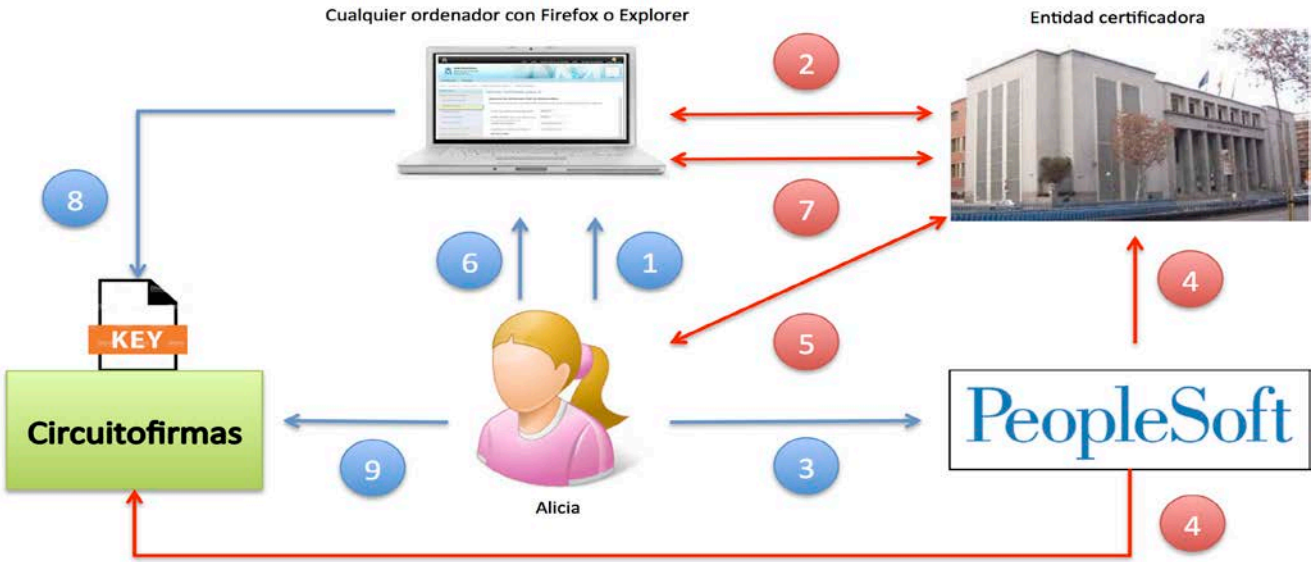
Documentación

- http://www.unizar.es/sede-electronica
- https://www.dnielectronico.es/PortalDNIe/
- PeopleSoft, Administración Electrónica, Ayuda

Firma en UNIZAR

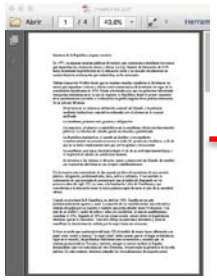
- Si no lo tenemos, **debemos solicitar certificado** personal o de empleado publico y, preferentemente, subirlo al servidor. Así podremos firmar desde cualquier dispositivo.
- Si eres “un tramitador”, necesitas disponer **del perfil para acceder HER@LDO-FIRMAS**. Solicitarlo a tramita@unizar.es
- Si eres “un firmante”, debes tener **cuenta en Circuitofirmas**. La cuenta se crea automáticamente al recibir la primera petición de firma.
- Si eres **personal externo a UNIZAR**, puedes solicitar cuenta en Circuitofirmas para facilitar la firma conjunta con personal interno. Por ejemplo un convenio de colaboración
- Podemos usar **la firma en escritorio** para asuntos particulares o para asuntos oficiales ya que nuestro sistema de gestión de documentos firmados (HER@LDO) admite la inclusión de un documento firmado externamente.
- Los documentos firmados en nombre de la **institución deben “subirse a custodia”** para asignarles un CSV y depositarlos en el sistema de validación. Esto solamente puede hacerlo un tramitador con el perfil adecuado.

Solicitud de certificado personal



1. **Alicia entra en la web de la FNMT con un navegador y solicita un certificado de empleado público**
2. El navegador genera un par de claves (privada y publica) y solicita la certificación de la clave pública.
   La FNMT recibe la solicitud y genera un código de solicitud que devuelve al navegador.
3. **Alicia entra en PeopleSoft, apartado *administración electrónica* e introduce el código de la solicitud.**
4. El personal de la Unidad People comunica a la FNMT la solicitud y envía el contrato de aceptación de condiciones para que lo firme Alicia en Circuitofirmas
5. La FNMT envía un mail a Alicia indicándole que ya puede descargar el certificado
6. **Alicia solicita la descarga del certificado (usando el mismo ordenador y navegador usado para hacer la solicitud).**
7. La FNMT envía el certificado al navegador que lo deposita en el almacén de certificados.
8. **Alicia hace una copia del certificado (junto con la clave privada) para usarlo en Circuitofirmasaplicación de firma**
9. **Alicia debe acceder a Circuitofirmas y firmar el documento recibido**

HER@LDO-Firma Genérica



DOCUMENTO ORIGINAL

cientia

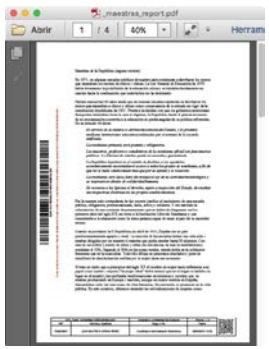
PLYCA contratación _ pública

HER@LDO -FIRMAS

CIRCUITOFIRMAS UNIZAR

DOCUMENTO FIRMADO PADES

CUSTODIA documentos UNIZAR

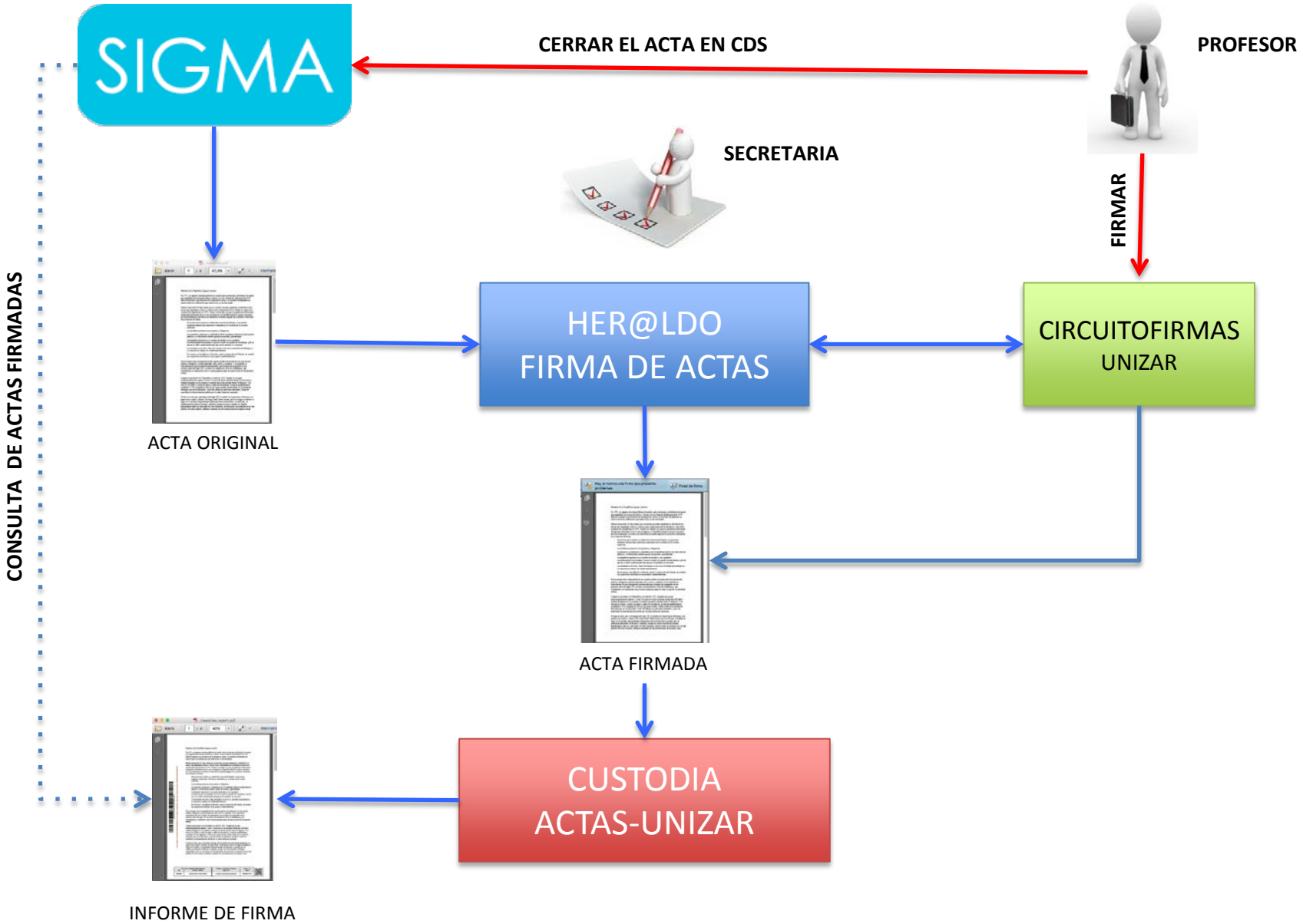


INFORME DE FIRMA

Publicación en TOUZ

Salidas/Envíos/Notificaciones

HER@LDO-Firma Actas



Universidad Zaragoza

Circuitofirmas
Plataforma ligera de firma digital

Configuración | Acciones | Carpetas | 04/05/2018 06:33:07 | 73096919K Pascual Perez Sanchez

- Configurar Usuario
- Comprobar certificado
- Comprobar firma
- Estadísticas de uso
- Ayuda
- Manual de usuario

dientes | En curso | Firmadas | Rech./Caduc./Retir. | Archivadas

Search:

			Estado	Docs.	Asunto	Firmantes
			caducada	2	Peticion creada en Circuito	73096919K Perez Sanchez, Pascual
		Normal	ustodiada	1	Acta de constitución comisión beca AE	04184380J Gil Costa, Alberto 25146773E Asensio Mera, Joaquin 73096919K Perez Sanchez, Pascual Marcelino
18315	2018-03-17 18:38:23	Normal	caduca	1	prueba backup online	73096919K Perez Sanchez, Pascual Marcelino

fnmt_pps.p12

Certificado Electrónico:

En este momento dispone de un certificado subido en 11-03-2018 08:35:20

Con este certificado podra realizar firmas aportando exclusivamente la contraseña de acceso. Esto le facilitará las tareas de firma desde dispositivos móviles.

Si lo desea, puede exportar este certificado para su utilizacion en otras aplicaciones, eliminarlo o sustituirlo por otro.

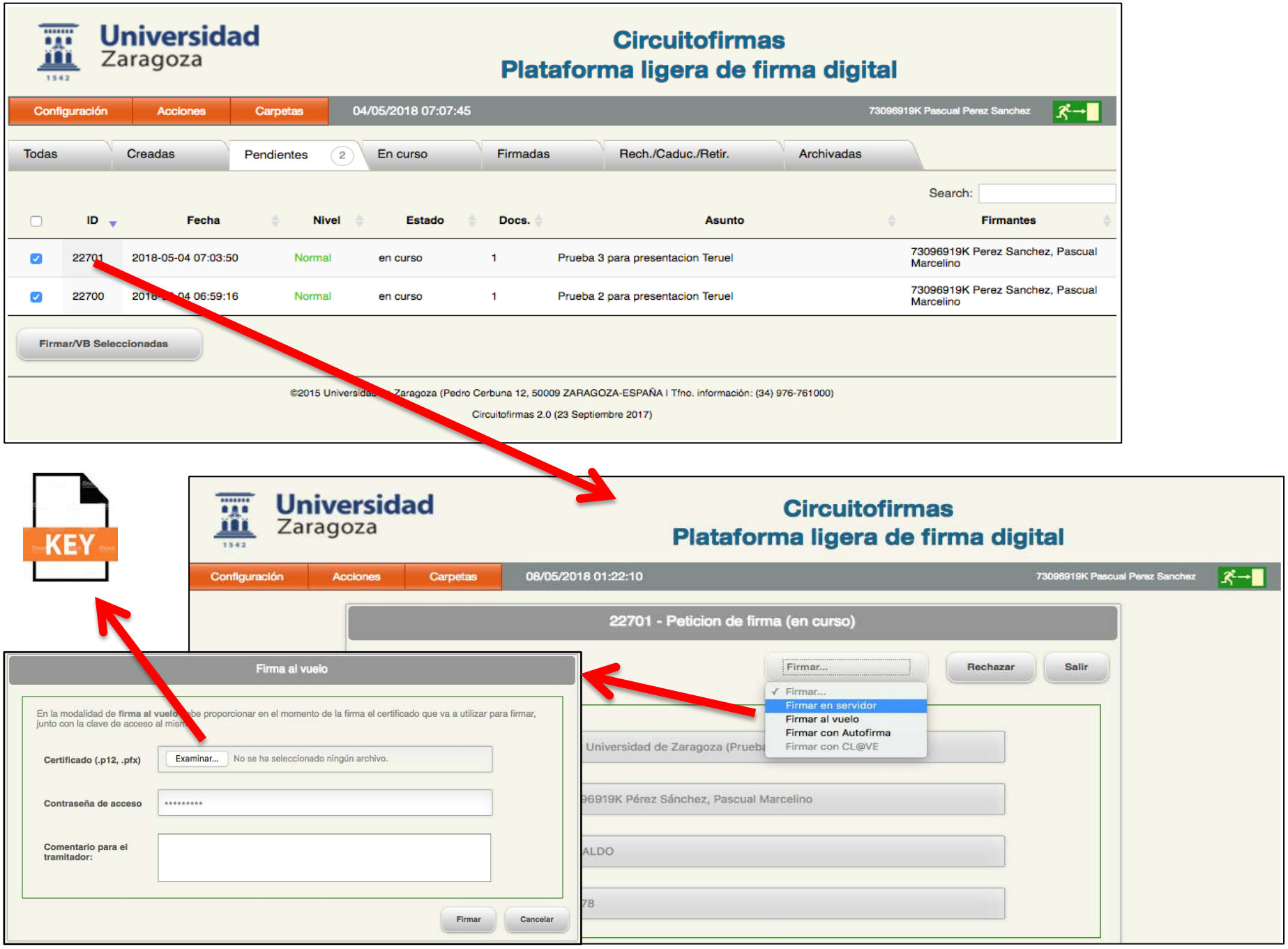
Certificado (.p12, .pfx) Examinar... No se ha seleccionado ningún archivo.

Contraseña Actual

Nueva Contraseña

Confirmar Contraseña

Importar | Exportar | Eliminar


Universidad Zaragoza
Circuitofirmas
Plataforma ligera de firma digital
Configuración
Acciones
Carpetas
04/05/2018 07:07:45
73096919K Pascual Perez Sanchez
Todas
Creadas
Pendientes 2
En curso
Firmadas
Rech./Caduc./Retir.
Archivadas
Search:
ID
Fecha
Nivel
Estado
Docs.
Asunto
Firmantes
22701 2018-05-04 07:03:50 Normal en curso 1 Prueba 3 para presentacion Teruel 73096919K Perez Sanchez, Pascual Marcelino
22700 2018-05-04 06:59:16 Normal en curso 1 Prueba 2 para presentacion Teruel 73096919K Perez Sanchez, Pascual Marcelino
Firmar/VB Seleccionadas
©2015 Universidad Zaragoza (Pedro Cerbuna 12, 50009 ZARAGOZA-ESPAÑA I Tfno. información: (34) 976-761000)
Circuitofirmas 2.0 (23 Septiembre 2017)
KEY
Universidad Zaragoza
Circuitofirmas
Plataforma ligera de firma digital
Configuración
Acciones
Carpetas
08/05/2018 01:22:10
73096919K Pascual Perez Sanchez
22701 - Peticion de firma (en curso)
Firmar...
Rechazar
Salir
Firmar...
Firmar en servidor
Firmar al vuelo
Firmar con Autofirma
Firmar con CL@VE
Universidad de Zaragoza (Prueba
96919K Pérez Sánchez, Pascual Marcelino
ALDO
78
Firma al vuelo
En la modalidad de firma al vuelo debe proporcionar en el momento de la firma el certificado que va a utilizar para firmar, junto con la clave de acceso al mismo
Certificado (.p12, .pfx)
Examinar...
No se ha seleccionado ningún archivo.
Contraseña de acceso
Comentario para el tramitador:
Firmar
Cancelar


That's all Folks!