Manual DNIe

Junio 2017

CONTENIDO DE LA JORNADA

El DNIe nos sirve para identificarnos. **No sólo en el mundo físico, sino también en el mundo virtual permitiendo realizar comunicaciones telemáticas seguras y firmar documentos electrónicos**. La firma electrónica que efectuamos usando el DNIe tiene los mismos efectos que la firma manuscrita. Resumiento: además de **identificarnos el DNIe nos permite**:

Acreditar electrónicamente y de forma inequívoca la identidad de la persona

Firmar digitalmente documentos electrónicos, otorgándoles una **validez jurídica** equivalente a la que les proporciona la firma manuscrita

El DNIe **incorpora un Chip** que contiene los mismos datos que aparecen impresos en la tarjeta (datos personales, fotografía, firma digitalizada, huella dactilar digitalizada) junto con **los certificados de Autenticación y de Firma Electrónica**

De esta forma, cualquier persona puede realizar múltiples gestiones online de forma segura con las Administraciones Públicas, con las empresas públicas y privadas y con otros ciudadanos, a cualquier hora y sin tener que desplazarse ni hacer colas. Podemos resumirlo con la frase:

"La Administración Electrónica 24 horas al día los 365 días a nuestra disposición"

El DNI 3.0 contiene antena NFC (Near Field Communication); es una **tecnología inalámbrica de corto alcance** que permite conectar dos dispositivos al emitir una señal, y que al mismo tiempo puede también recibir una señal. Permite, por lo tanto, una lectura-escritura en ambos sentidos. El NFC opera en la frecuencia de 13.56 MHz y permite una distancia inferior a los 10 cm (**los dispositivos NFC tienen que tocarse prácticamente para poder hacer la transmisión de datos**). Funciona a una velocidad de hasta 424 kbit/s de transmisión y tarda alrededor de 200 microsegundos en establecer un enlace NFC.

CARACTERÍSTICAS DEL DNIE

CARACTERÍSTICAS FÍSICAS DNI2.0:

La tarjeta soporte del DNI electrónico es de policarbonato, un material muy resistente, de alta calidad y durabilidad, que permite el grabado de los datos con láser destructivo, lo que hace virtualmente imposible falsificar la impresión.

- El Documento Nacional de Identidad tiene impresos los siguientes datos de filiación del titular:

  - Apellidos y nombre
  - Sexo
  - Nacionalidad
  - Fecha de nacimiento

- La fotografía, en blanco y negro, tiene un holograma en la superficie.
  Relieves.

Holografía: La holografía es una técnica avanzada de fotografía, que consiste en crear imágenes tridimensionales. Para esto se utiliza un rayo láser, que graba microscópicamente una película fotosensible. Ésta, al recibir la luz desde la perspectiva adecuada, proyecta una imagen en tres dimensiones. **Fuente**: wikipedia

- Número personal del Documento Nacional de Identidad y carácter de verificación.

- Firma manuscrita del titular.

- · Número de serie del soporte.
- · Fecha de validez del documento.

- Imagen cambiante grabada en láser.

CARACTERÍSTICAS ELECTRÓNICAS

El nuevo Documento Nacional de Identidad dispondrá de un chip electrónico en el que se almacenarán los datos del titular.

- Datos de filiación del titular
- Imagen digitalizada de la fotografía
- Imagen digitalizada de la firma manuscrita
- Plantilla de la impresión dactilar
- Certificado reconocido de autentificación y de firma
- Certificado electrónico de la autoridad emisora
- Par de claves de cada certificado electrónico

Caracteres OCR-B de lectura automática por máquinas. Esta zona se divide en 3 campos:

(Voy a utilizar un ejemplo de datos diferente a la captura de pantalla referente)

IDESPABC123456012345678Z<<<<<<
7410150M0903226ESP<<<<<<<<<<<9
DE<TAL<Y<CUAL<<FULANITO<<<<<<<

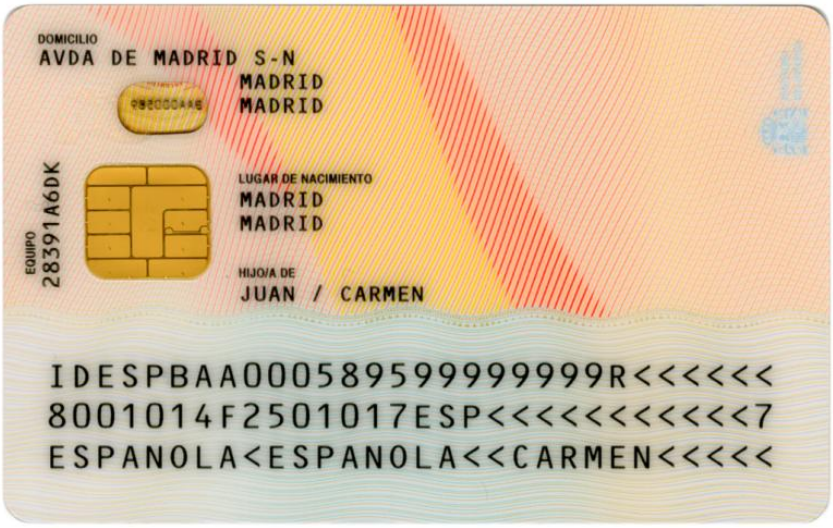
1.[ID]
2.[ESP]
3.[ABC123456]
4.[0]
5.[12345678Z]
6.[<<<<<<]

7.[741015]
8.[0]
9.[M]
10.[090322]
11.[6]
12.[ESP]
13.[<<<<<<<<<<<]
14.[9]
15.[DE<TAL<Y<CUAL<<FULANITO<<<<<<<]

1. Tipo de documento
2. Nación
3. Número de serie del soporte físico de la tarjeta
4. Dígito de control del campo 3
5. Número de DNI
6. Relleno
7. Fecha de nacimiento (AÑO MES DÍA)
8. Dígito de control del campo 7
9. Sexo (M/F)
10. Fecha de caducidad
11. Dígito de control del campo 10
12. Nacionalidad
13. Relleno
14. Dígito de control de los campos 3, 4, 5, 7, 8, 10 y 11 concatenados
15. Nombre

CARACTERÍSTICAS FÍSICAS DNI 3.0: (info dnielectronico.es)

El Chip del DNI 3.0 está localizado en la parte izquierda del **reverso de la tarjeta**. Es una **tarjeta que es capaz de emitir datos que pueden ser leídos** por un funcionario del estado (policía) **desde otro dispositivo** con el hardware y el software requerido



Características:

400KB memoria Flash (código + personalización)

8 KB memoria RAM

Dual Interface: conexión mediante hardware y de forma inalámbrica con la tecnología NFC. Para utilizar la funcionalidad inalámbrica del DNI 3.0 únicamente será necesario disponer de:

- **Un teléfono Smartphone o tablet con tecnología NFC.**
- **App del servicio al que nos queremos conectar.**

El ciudadano no tendrá por tanto, que descargarse ningún certificado o driver, sino que **la conexión se iniciará simplemente con acercar el DNI 3.0 a la antena NFC del dispositivo**, (a una distancia no superior a 1 cm).

Criptolibrería RSA

CC EAL5+

Contenido del chip: La información en el chip está distribuida en dos zonas con diferentes niveles y condiciones de acceso:

Zona pública: Accesible en lectura sin restricciones, contenido:

Certificado CA intermedia emisora

Claves Diffie-Hellman

Certificado x509 de componente

Certificado de Firma

Certificado de Autenticación

Zona de seguridad: Accesible en lectura por el ciudadano, en los Puntos de Actualización del DNI.

Datos de filiación del ciudadano (los mismos que están impresos en el soporte físico)

Imagen de la fotografía.

Imagen de la firma manuscrita.

CRIPTOGRÁFICOS: Claves de ciudadano:

Clave RSA pública de autenticación (Digital Signature)

Clave RSA pública de no repudio (ContentCommitment).

Clave RSA privada de autenticación (Digital Signature).

Clave RSA privada de firma (ContentCommitment).

Patrón de impresión dactilar.

Clave Pública de root CA para certificados card-verificables.

Claves Diffie-Hellman.

DATOS de GESTIÓN:

Traza de fabricación.

Número de serie del soporte.

CERTIFICADOS ELECTRÓNICOS

Un certificado electrónico es un documento que identifica a una persona. **El DNI lleva asociado la correspondiente obtención de los certificados electrónicos de Autenticación y de Firma Electrónica**.

Certificado de autenticación: Garantiza la identidad del ciudadano al realizar un trámite o comunicación a través de la red

Certificado de firma: Permite firmar trámites o documentos a través de la red, sustituyendo de esta forma la firma manuscrita

RENOVACIÓN CERTIFICADOS (info dnielectronico.es)

Renovación de claves sin renovación del soporte físico (tarjeta):

La renovación de las claves es voluntaria, gratuita y por iniciativa del ciudadano.

En fechas próximas a la caducidad de sus certificados, recibirá, en la cuenta de correo electrónico que usted haya proporcionado en el momento de la expedición de su DNI, un aviso procedente de la dirección oficial notificaciones@policia.es, en el que le advierten de la próxima caducidad de sus certificados electrónicos.

El titular puede proceder a renovar los certificados, si el estado de los mismos es uno de los siguientes:

Si fueron revocados a petición del ciudadano (solo podrá revocarse el certificado de firma digital).

Por caducidad. Los certificados electrónicos incorporados en **el DNI tendrán un período de vigencia de 30 meses**, y los contenidos en el **DNI 3.0 tendrán un periodo de vigencia de hasta 60 meses (mejora de notoria importancia, puesto que la anterior regulación los limitaba a 30 meses y solo se podían renovar una vez caducados o dentro de los 30 días de la fecha de caducidad**.

Para proceder a la renovación deberá mediar la presencia física del titular en una Oficina de expedición. El ciudadano, haciendo uso de los Puntos de Actualización del DNIe habilitados en dichas oficinas y previa autenticación mediante la tarjeta y las plantillas biométricas (impresiones dactilares) capturadas durante la expedición de la Tarjeta, podrá desencadenar de forma desatendida el proceso de renovación de sus certificados.

EL PROCESO DE RENOVACIÓN DE CERTIFICADOS EN EL PUNTO DE ACTUALIZACIÓN DEL DNI 3.0 ES EL SIGUIENTE:

El titular tras introducir correctamente el PIN, accede a la pantalla de "información sobre el contenido de su DNI 3.0", en la parte inferior puede visualizar el estado de sus certificados. En su caso, en la parte izquierda aparece una casilla "renovar certificados". Si se selecciona "renovar certificados" solicita nuevamente el PIN y posteriormente la presentación de la huella dactilar. Si el resultado es positivo se procede a la renovación de los certificados; este proceso dura aproximadamente 3 minutos. Es importante, no retirar el documento del lector de tarjetas hasta la finalización del proceso, porque el DNIe podría quedar inservible. Si no fuere posible obtener la impresión dactilar de alguno de los dedos, el ciudadano deberá solicitar la renovación en un puesto de expedición atendido por un funcionario.

En el caso que haya transcurrido más de 5 años desde la identificación inicial del ciudadano (es el caso de la segunda renovación de los certificados en soportes de 10 o más años), en cumplimiento del artículo 13 de la Ley de Firma Electrónica (“La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará …”) la renovación a través de los

Puntos de Actualización del DNI 3.0 requerirán la personación previa del ciudadano ante un funcionario de la Oficina de Expedición a los efectos del mencionado artículo.

No se habilita, por tanto, **ningún procedimiento para solicitar de forma telemática la renovación de los certificados siendo necesaria en todos los casos la presencia física del titular**

FIRMA ELECTRÓNICA

La firma electrónica, como su propio nombre indica, es el equivalente electrónico de nuestra firma manuscrita.

Sus principales funciones son:

- Identificación del firmante: la firma identifica al firmante de forma única igual que su firma manuscrita.

- **Integridad del contenido firmado**: es posible verificar que los documentos firmados no hayan sido alterados por terceras partes.

- **No repudio del firmante**: un documento firmado electrónicamente no puede repudiarse por parte de su firmante.

- Es un conjunto de datos que nos **permiten acreditarnos** y cerrar acuerdos por medios electrónicos, principalmente por Internet.

- En España, **desde el año 2003**, **la firma electrónica tiene el mismo valor a efectos legales que la firma manuscrita**. (LEY 59/2003, del 19 de diciembre, de firma electrónica)

Autoridades de Validación

La Autoridad de Validación es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación

Para la validación del DNI se dispone de dos prestadores de Servicios de Validación:

Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, que prestará sus servicios de validación a ciudadanos, empresas y Administraciones Públicas.

Ministerio de Hacienda y Administraciones Públicas, que prestará los servicios de validación al conjunto de las Administraciones Públicas.

¿Qué necesito para usar el DNIe?

Para usarlo necesitas disponer de un lector de **DNIe** y del software necesario y un pc con acceso a internet

Si dispones de un lector USB sigue los pasos recomendados por el fabricante para instalarlo. Normalmente:

Conectar el lector al Pc

Descargas los drivers del lector

Instalas el software del **DNIe**

En cuanto al software necesario para utilizar el **DNIe**, el enlace para la descarga es el siguiente:

http://www.dnilectronico.es/

Una vez descargado e instalado el software que nos permita interactuar con nuestro **DNIe** necesitamos configurar nuestro lector de tarjetas, en nuestro caso tenemos el lector integrado en el teclado. En caso de no ser así conectaríamos nuestro lector USB al Pc y seguimos las instrucciones recomendadas por el fabricante del dispositivo. En algunos casos es necesario instalar un driver específico que varía en función del modelo de lector y del sistema operativo

Una vez instalado el software de **DNIe** y configurado el lector podemos empezar a usar el **DNIe**

Insertamos el **DNIe** en el lector y acto seguido nos pedirá el **PIN**, nos lo entregan en sobre ciego junto con el **DNIe** en el momento de la expedición.

Podemos cambiar el **PIN** que nos entregan en los puntos de expedición del **DNIe**. Introducimos el **DNIe** en la máquina y seguimos las indicaciones.

Recomendaciones a la hora de cambiar el **PIN**:

Debes elegir un **PIN** de una longitud entre 8 y 16 caracteres alfanuméricos.

Debes elegir un **PIN** que sea fácil de recordar, para no tener que escribirlo.

No es aconsejable emplear como **PIN** su nombre o apellidos (o de familiares) o una derivación de éstos.

No conviene utilizar como **PIN** datos relacionados con usted que puedan obtenerse fácilmente (número de teléfono, matrícula del vehículo, dirección postal).

Hay que evitar utilizar como **PIN** secuencias repetidas de números (o letras).

Lo ideal es utilizar una combinación de letras (mayúsculas y minúsculas) y números.

3.0 SISTEMAS OPERATIVOS, DISPOSITIVOS PARA EL DNI 3.0

El DNI electrónico requiere el siguiente equipamiento físico:

- Un Ordenador personal (Intel -a partir de Pentium III- o tecnología similar).
- Un lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una interfaz PCMCIA.

  Para elegir un lector que sean compatible con el DNI electrónico, verifique que, al menos:

  - ✓ Cumpla el estándar ISO 7816 (1, 2 y 3)
  - ✓ Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1)
  - ✓ Soporta velocidades de comunicación mínimas de 9.600 bps.
  - ✓ Soporta los estándares:
    - API PC/SC (Personal Computer/Smart Card)

B. Elementos software para PC

- Sistemas operativos

  El DNI electrónico puede operar en diversos entornos:

  - Windows 7 y superioresGNU/Linux
  - Unix
  - Mac

- Navegadores

  El DNI electrónico es compatible con todos los navegadores:

  - Microsoft Internet Explorer
  - Chrome
  - Mozilla Firefox

- Controlador del Lector

  - Para operar con un lector de tarjetas inteligentes, será necesario instalar un driver que, normalmente, se distribuye con el propio lector

- Controladores / Módulos criptográficos de la tarjeta DNIe

  Para poder interaccionar adecuadamente con las tarjetas criptográficas en general y con el DNI electrónico en particular, el equipo ha de tener instalados unas "piezas" de software denominadas módulos criptográficos.En un entorno Microsoft Windows, el equipo debe tener instalado driver denominado Minidriver o CardModule y PKCS#11En los entornos UNIX / Linux o MAC podemos utilizar el DNI electrónico a través de un módulo criptográfico denominado PKCS#11

- Instalacion automática CardModule

  Para aplicativos Microsoft como Internet Explorer o para Chrome basta con tener el equipo conectado a Internet e insertar la tarjeta en el lector. El servicio Windows Update buscará automáticamente el driver de la tarjeta y lo instalará. Se trata de un dispositivo Plug & Play

  http://www.dnie.es/PDFs/Explorer%20y%20Chrome.pdf

- Instalación manual CardModule

  Si por cualquier razón no se puede realizar la instalación automática, hay disponible un instalable para realizar la instalación de modo manual http://www.dnielectronico.es/descargas/historico.html

- Instalación PCKS11

Para instalar el módulo criptográfico PKCS11 se deben seguir las recomendaciones http://www.dnie.es/PDFs/Familia%20Mozilla.pdf

Mediante antena sin contactos NFC

A. Elementos hardware

- Un dispositivo con NFC que cumpla el estándar ISO 14443, tipo A o B, ya que el DNI 3.0 es compatible con ambas implementaciones del estándar ISO 14443. Este puede ser un Smartphone, una tableta o un lector NFC. Para elegir un dispositivo compatible con el DNI electrónico, verifique que cumple:

  - ISO 14443 - Partes 1/2/3/4. Protocolo de transmisión T=CL

B. Elementos software

- APP que use el DNIe para identificarse y así acceder a un servicio específico o para realizar firmas de documentos.

  Para su instalación habrá que acceder al repositorio de APP (Google Play….) y proceder a su descarga e instalación. Otra opción es que la propia entidad u organismo lo tenga disponible en su portal WEB.

COMPRUEBA TU DNIe

Desde este apartado puedes verificar el estado de los certificados instalados en tu **DNIe**. **Caducan a los 30 meses y desde 2015 los certificados que incorpora el DNI tienen una validez de 5 años (60 meses)**

Se han de renovar en uno de los puntos habilitados para ello. Si los certificados están caducados no puedes utilizar tu **DNIe**. Enlace para comprobar el estado de los certificados:

http://www.dnielectronico.es/como_utilizar_el_dnie/verificar.html

VENTAJAS

Facilita las relaciones entre ciudadanos, empresas y administraciones.

"La tecnología nos hace la vida más fácil"

El DNI electrónico ofrece la posibilidad de aprovechar el tiempo realizando multitud de trámites por vía telemática, de forma que:

Se evitan desplazamientos

Los trámites se pueden realizar en cualquier momento, adaptándose a nuestros horarios

Las gestiones se llevan a cabo de manera sencilla, siguiendo las indicaciones de cada uno de los Organismos públicos y privados

Desde el punto de vista de la seguridad, el DNI electrónico es más seguro que el tradicional, ya que incorpora mayores y más sofisticadas medidas de seguridad que hacen imposible su falsificación. Asimismo, permite garantizar la identidad de los interlocutores de una comunicación online, ya sea para intercambio de información, acceso a datos o acciones o compra por Internet, a la vez que asegura que la información intercambiada no ha sido alterada.

Además, todo son facilidades para su obtención y utilización:

Se expide de forma inmediata, a través de cita previa.

Tiene las mismas medidas que el anterior DNI, pero de un material mucho más robusto y duradero.

Se facilita el código **PIN** y la posibilidad de cambiarlo en la oficina (El **PIN** es lo que protege la información que contiene el **DNIe**: los **certificados de autentificación y de firma electrónica**, así como sus respectivas claves privadas y públicas)

Está aceptado por parte de todas las administraciones públicas (lo podemos usar para pedir un certificado de empadronamiento, hacer la declaración de la renta, dar de alta en el registro de nacimientos o consultar un informe de vida laboral)

PASOS PARA CAMBIAR EL PIN

Actualmente **NO ES POSIBLE cambiar el PIN a través de Internet**, siendo necesario acudir físicamente a una Oficina de expedición para poder realizar esta operación.

TRÁMITES DISPONIBLES CON EL DNI-e

Con la administración central: Las administraciones disponen de trámites para realizar online

Presentarse a ofertas de empleo público

Solicitar la devolución de gasóleo agrícola

Obtener un informe de vida laboral

Información de retenciones e ingresos a cuenta del IRPF. Para las personas que han percibido prestaciones de la Seguridad Social

Personas interesadas en recibir información de las subastas convocadas para la venta de inmuebles pertenecientes a la Tesorería General de la Seguridad Social

Consultar las bases de cotización

Solicitud cambio de domicilio

Comunicación de teléfono móvil y correo electrónico

Informe de datos identificativos y de domicilio

Solicitar la prestación por desempleo

Trámites con la agencia tributaria

Con la administración autonómica: www.asturias.es

Ayudas para la renovación de instalaciones eléctricas de baja tensión

Ayudas a proveedores de productos lácteos a centros escolares

Ayudas para la obtención de productos orto-protésicos

Ayudas al alquiler joven (renta básica de emancipación)

Apoyar a las trabajadoras autónomas que por motivos de maternidad, adopción, o acogimiento preadoptivo, necesiten contratar a una persona que les permita disfrutar de permisos por dichas causas

Solicitud de subvenciones

Solicitar el carné de familia numerosa

Iniciar la actividad como establecimientos hoteleros (hoteles) y proceder a su clasificación

Solicitud de alta, renovación, cambio de titularidad o baja del Registro de una explotación agraria

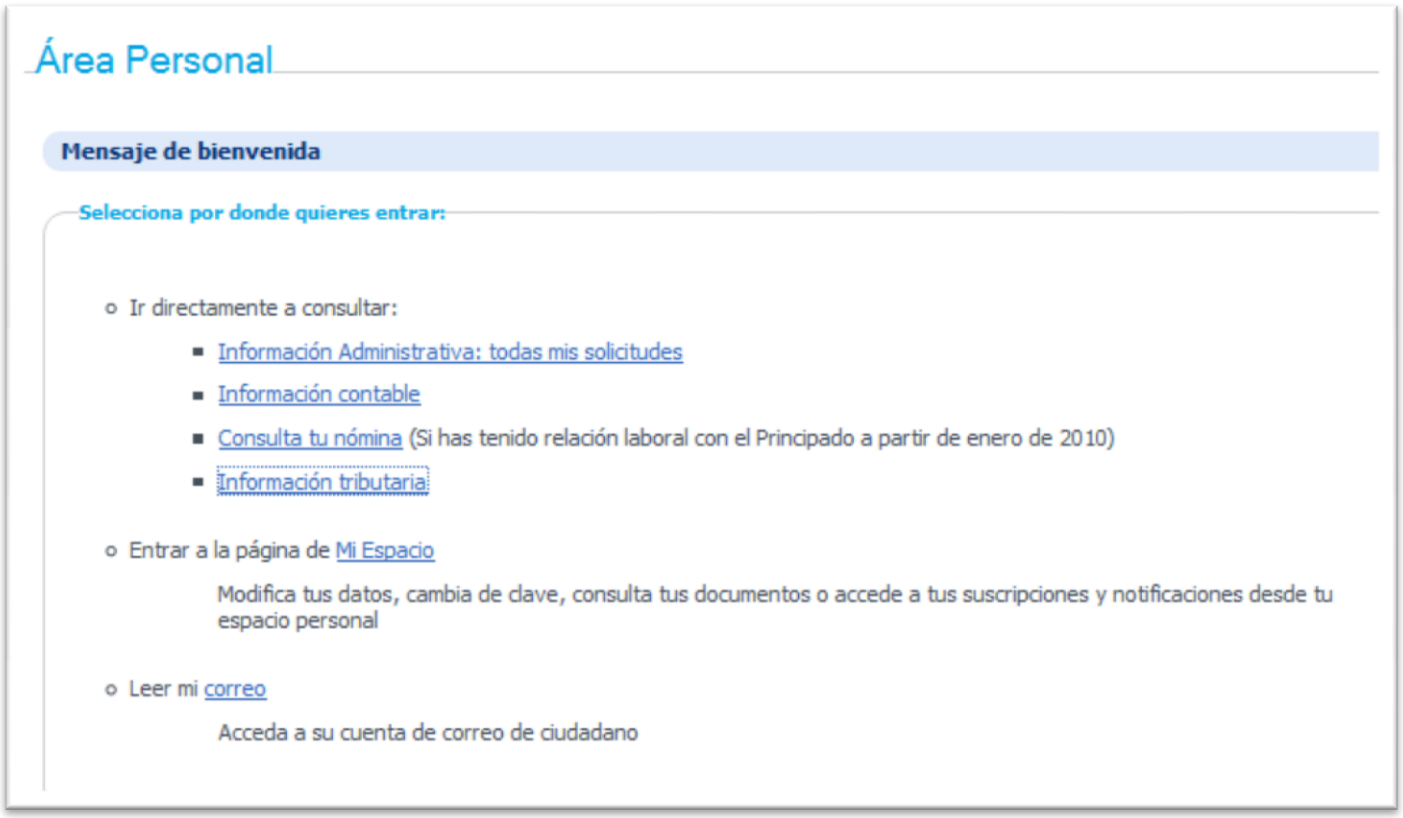
Renovar la demanda de empleo

Inserción de textos en el Boletín Oficial del Principado de Asturias (BOPA)

Consulta de notas académicas on-line si eres tutor legal de un alumno/a matriculado en un centro educativo.

Consulta de datos del alumnado: Desde aquí podrás ver los datos de las fichas del alumnado matriculado en los centros educativos del Principado de Asturias y, si eres tutor, podrás actualizar los datos.

Acceder al área personal y consultar el estado de tus tramitaciones. Una vez que te validas con tu DNIe accedes a esta pantalla para seleccionar la información que necesitas consultar



Desde el enlace "información tributaria" accedes al portal tributario del Principado desde entre otras cosas puedes realizar el pago de la viñeta del vehículo hasta obtener un duplicado del recibo del año anterior

Administración Local

http://sedeelectronica.grandasdesalime.es

Para iniciar cualquier trámite es requisito identificarse digitalmente. El medio válido de identificación con la sede electrónica del Ayuntamiento de Grandas de Salime es el Certificado de la FNMT (Solicitar un certificado de empadronamiento) y el DNIe. Con Windows xp funciona mejor la conexión a la sede electrónica con Mozilla firefox, chrome presenta problemas puesto que chrome ha dejado de soportar algunos plugins necesarios para acceder a la sede electrónica

Presentación de solicitudes, escritos y comunicaciones, verificación de documentos electrónicos y otros servicios relacionados con la entrega y validación de documentación electrónica.

CASOS PRÁCTICOS con el DNIe

COMPROBAR LA VALIDEZ DE LOS CERTIFICADOS

TRÁMITES:

Seguridad Social:

Informe de vida laboral

Consulta de bases de cotización

Solicitud de cambio de domicilio

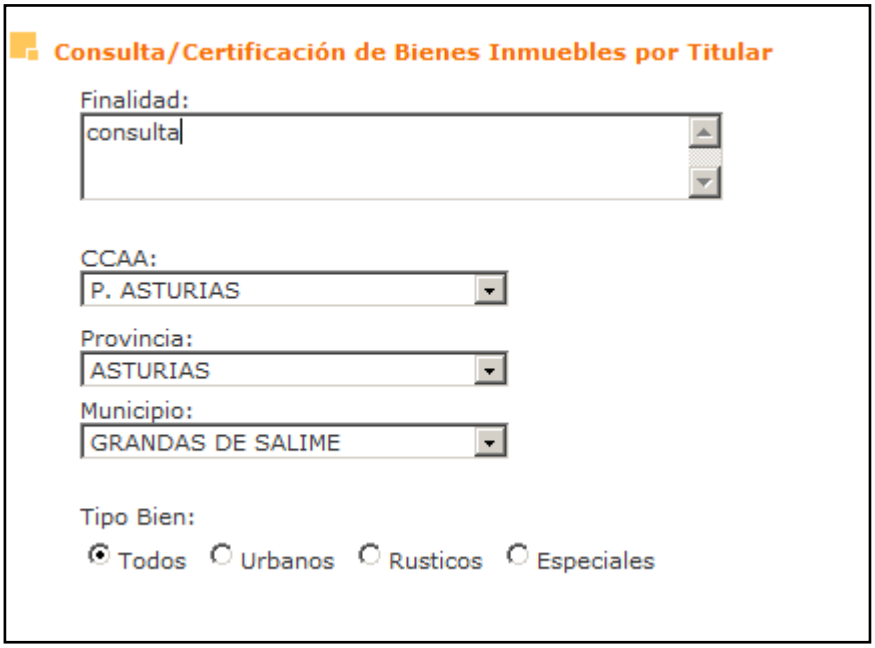
Informe de situación actual del trabajador

http://administracion.gob.es/

- Consulta de datos catastrales

Consulta de los datos catastrales que figuran a tu nombre (en caso que no tengas inmuebles a tu nombre también lo indica)

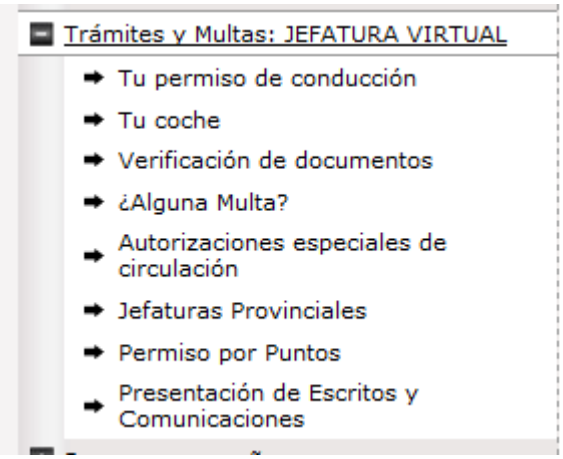
Nos muestra un formulario para rellenar



DGT.es

Permiso por puntos

Pago de multas



Accedemos a este catálogo de servicios:

DEV: Darse de alta en la DEV implica dos pasos: primero suscribirse a la DEV rellenando el formulario, disponible en Internet, y después, suscribirse a los tipos de comunicaciones y avisos que desee, dentro de los disponibles.

Importante: Suscribirse a la DEV implica que todas las Administraciones con competencia en materia de Tráfico (Comunidades Autónomas y Ayuntamientos) le notificarán también vía Internet.

EI TESTRA (Tablón Edictal de Sanciones de Tráfico) es un tablón electrónico que le permite consultar las notificaciones por sanciones de Tráfico que no hayan podido practicarse en el domicilio del interesado por estar éste ausente, por haber cambiado de domicilio sin haberlo comunicado, etc.

Pago de multas, notificación de multas por internet, identificación del conductor

Acceder a la banca online

FIRMA

La firma electrónica es un concepto más amplio que el caso de la digital. Mientras que el segundo hace referencia a una serie de métodos criptográficos, el concepto de firma electrónica es de naturaleza fundamentalmente legal, ya que confiere a la firma un marco normativo que le otorga su validez jurídica.

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

Identificar al firmante de manera inequívoca.

Asegurar la integridad del documento firmado, asegurando que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación alguna en el tiempo.

Asegurar que el firmante no puede repudiar lo firmado.

La base legal de la firma electrónica está recogida en la Ley 59/2003. Para firmar un documento es necesario disponer de un certificado digital o de un DNI electrónico. El certificado electrónico o el DNI electrónico contienen unas claves criptográficas que son los elementos necesarios para firmar.

Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor y son emitidos por proveedores de servicios de certificación.

El proceso básico a seguir para firmar electrónicamente, es el siguiente:

- El usuario dispone de un documento como puede ser una hoja de cálculo, un pdf, una imagen y de un certificado electrónico que le pertenece y le identifica.
- La aplicación o dispositivo digital utilizados para firmar, realiza un resumen del documento. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
- La aplicación utiliza la clave contenida en el certificado electrónico para codificar el resumen.
- La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.
- El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante. La firma electrónica, por tanto, es el mismo documento electrónico resultante.

FIRMAR UN DOCUMENTO

Para firmar un documento en forma electrónica debe realizarse, de forma obligatoria, utilizando medios electrónicos y esto se puede hacer de dos maneras:

- Descargando una aplicación en modo local en un ordenador:
    - En este caso se utiliza para firmar la aplicación que se ha instalado en modo local. Las aplicaciones que podemos descargar son el Cliente **@Firma** del Ministerio de Política Territorial o **ecoFirma** del Ministerio de Industria, Reemplazado por **Autofirma**. Podemos

obtener más información sobre ellas y realizar las descarga respectivas en aplicaciones para firmar de manera electrónica o en el servicio de validación de Sede Electrónica de VALIDe

- Firmar directamente en internet:
  - Esta opción es usada sobre todo cuando se firman formularios o solicitudes, por ejemplo, en la relación con la administración pública.
  - También se puede firmar documentos propios en internet, realizando los pasos siguientes:
    - Acceder al https://valide.redsara.es/valide/firmar/ejecutar.html
    - Pulsar el botón 'Firmar'.
    - Seleccionar el documento.
    - Pulsar el botón 'Guardar la firma'.

En ambos casos necesitamos disponer de un certificado electrónico.

Debemos tener presente que el documento original está incluido en el nuevo fichero electrónico de firma

Firmar de forma electrónica, aporta **tres características** en la comunicación por Internet:

- **Identificar** al firmante.
- **Integridad** de los datos.
- Asegurar el **no repudio**.

Verificar un documento firmado

Si recibimos un documento firmado podemos validar su firma, lo que es lo mismo, comprobar que los datos firmados se corresponden con los originales, que el certificado electrónico con el que se ha firmado es válido y que la estructura del fichero es correcta.

La validación de una firma electrónica es el proceso por el que se comprueba:

- La identidad del firmante.
- La integridad del documento firmado.
- La validez del certificado utilizado.

Podemos comprobar la validez de la firma de un documento, ver quién es el firmante y el documento firmado en la Sede Electrónica de VALIDe, realizando los pasos siguientes:

- Acceder al servicio de validación de Sede Electrónica de VALIDe.
- Seleccionar un archivo.
- Introducir el código de seguridad.
- Pulsar el botón Valida

HERRAMIENTAS DE FIRMA

Con el DNIe además de realizar trámites con la administración también podemos firmar documentos.

Nombramos 3 programas:

Adobe acrobat PRO, versión comercial

Xolidosign, gratuito

Autofirma, gratuito

XOLIDOSIGN

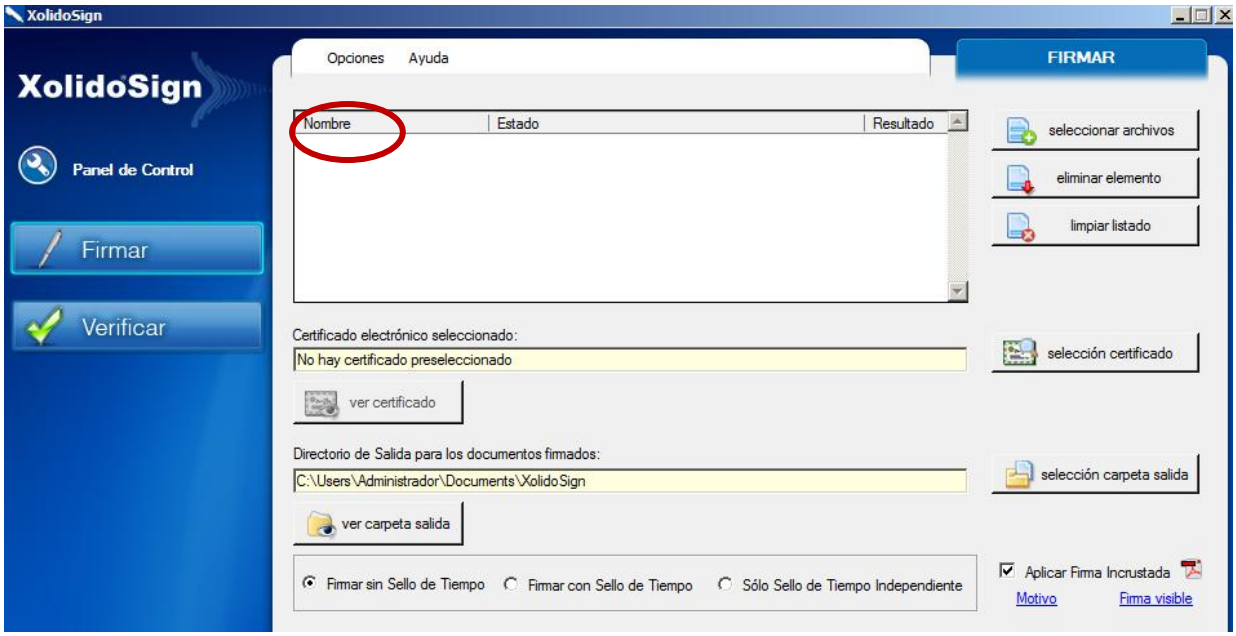
Aplicación que me permite **firmar digitalmente los documentos y comprobar la autenticidad** (verificar que los documentos no han sido manipulados). Permite sellado de tiempo de esta forma el usuario puede acreditar el día y la hora en que un archivo fue recibido o enviado

Enlace a la aplicación:http://www.xolido.com/lang/productosyservicios/firmaelectronicayselladodetiempo/xolidosignsuite/index.shtml

Sirve para firmar documentos en:

PDF, Word, Excel…

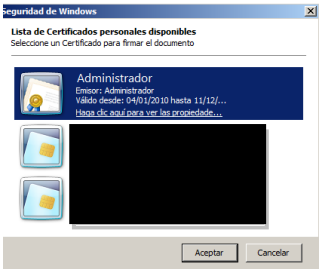
Una vez instada la aplicación accedemos a ella desde el acceso directo instalado en el escritorio



Una vez abierto el programa clicas en firmar y te muestra esta ventana

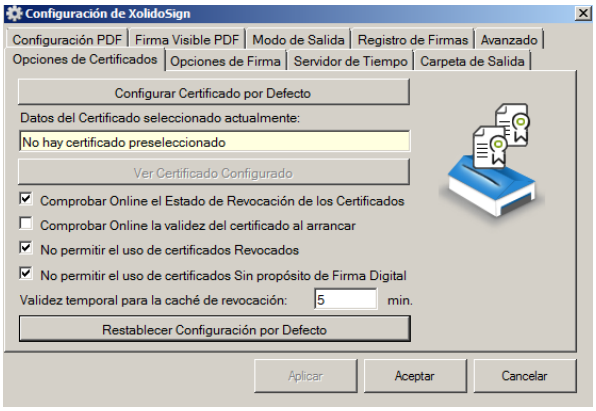
Accedemos a las opciones de configuración del programa a través de **opciones, configuración:**

Podemos configurar el certificado que se usa por defecto, en caso que se tenga instalado más de un certificado. Accedemos a la lista de certificados instalados y elegimos el que se usa por defecto:

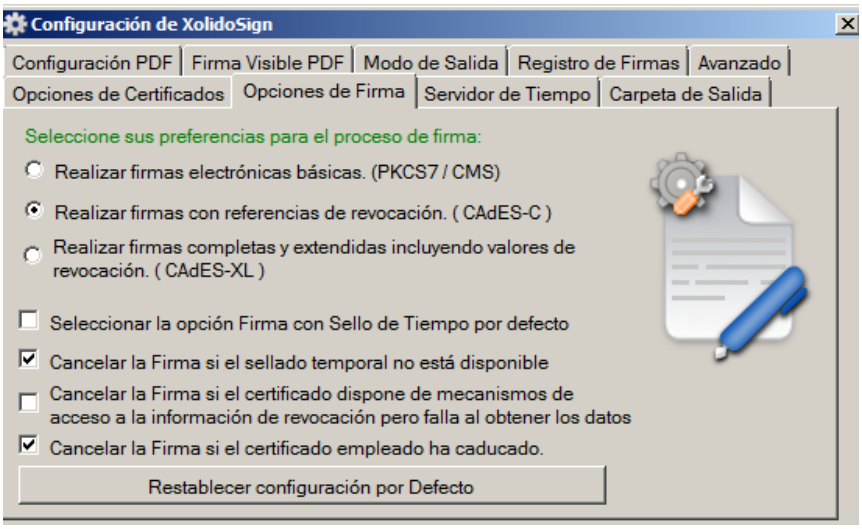


Por defecto la aplicación realiza la comprobación online del estado de revocación de los certificados

Dejamos activadas estas opciones:

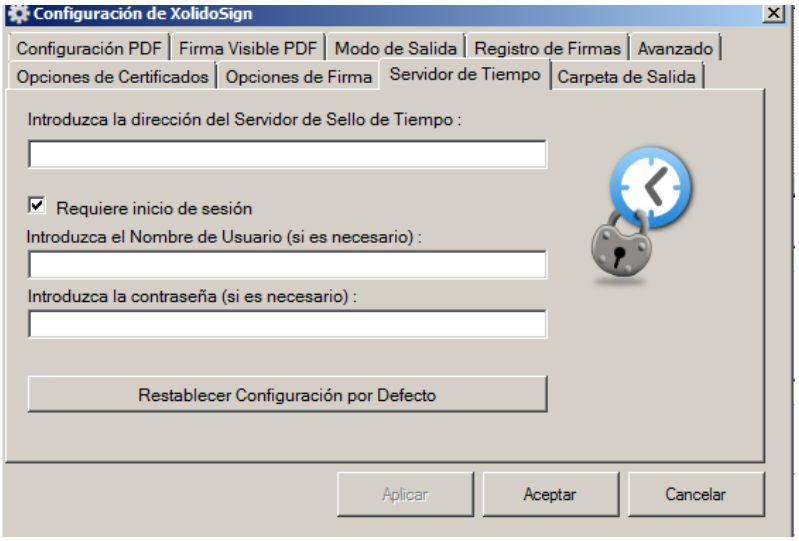


Opciones de firma, habitualmente se utiliza la firma electrónica básica

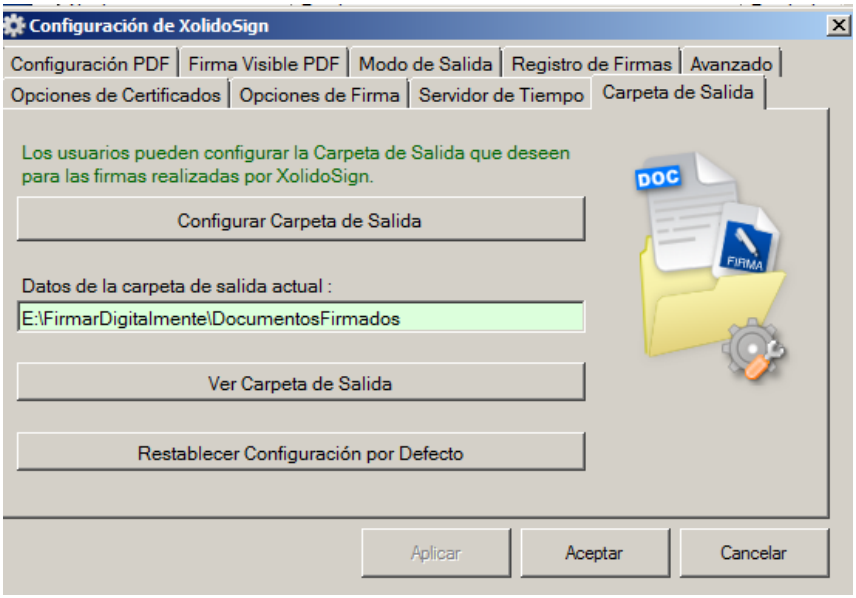


Elegimos el tipo de firma electrónica que se utilizará

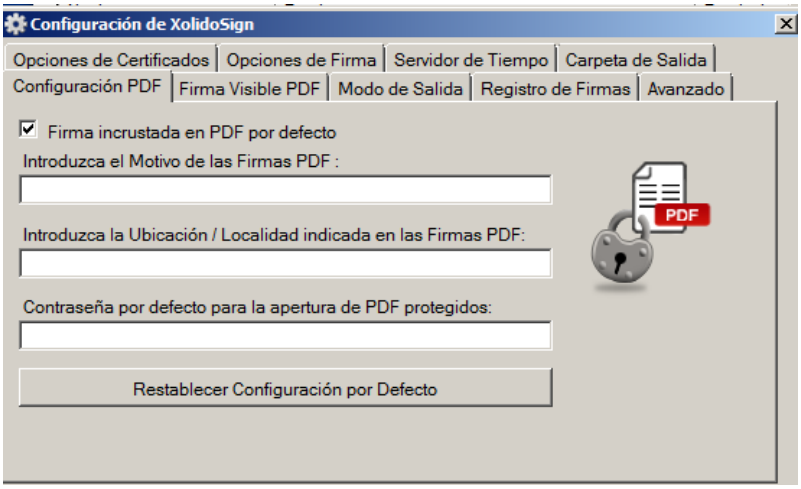
Firmado con Sello de tiempo. Nos indicará la fecha de creación o modificación de un documento o firma electrónica. Nos pedirá la ruta de acceso al servidor, usuario y contraseña



Indicamos la carpeta donde se almacenarán los documentos firmados



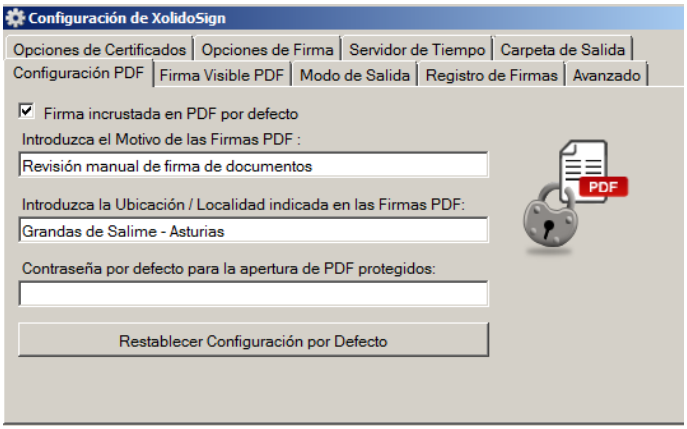
Configuramos la firma para los documentos en PDF



Por defecto la firma se incrusta en el propio documento PDF que se firma (posteriormente al abrir el PDF firmado podemos ver, mostrar la firma en la parte del PDF que le indiquemos).

Podemos indicar un motivo de firma, se indica la razón por la que se procede a firmar el documento (revisión, aprobación, etc).

La ubicación de las firmas hace referencia a la ubicación geográfica que se desea mostrar para las firmas incrustadas. En ambos casos son valores informativos



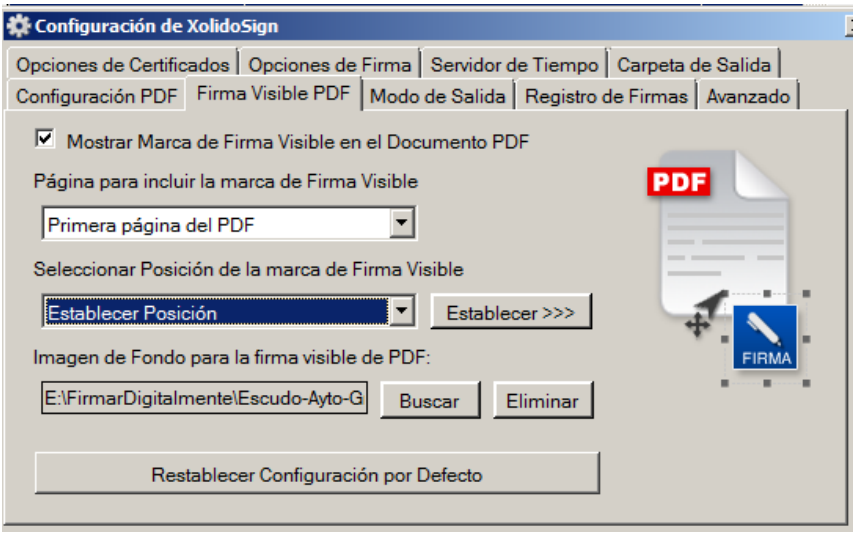
FIRMA VISIBLE PDF

Hace referencia a la localización de una firma incrustada en PDF dentro del documento. Si activamos la opción “mostrar marca de firma visible en el documento PDF” podemos elegir:

La página en la que se muestre la firma que puede ser:

En la primera página / en la última página o en la página que nosotros indiquemos del documento

Podemos indicar la posición donde se inserte la firma y una imagen de fondo para la firma que puede ser el logo de la entidad



Modo de salida

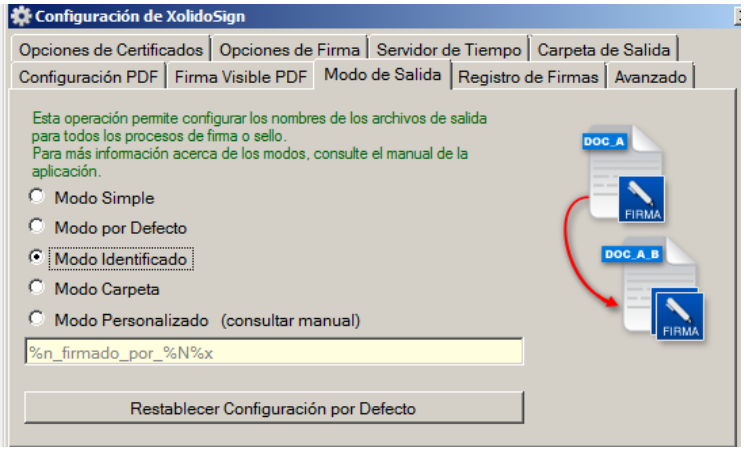
Desde esta pestaña configuramos el nombre que se va asignar al documento firmado:

Modo simple: el archivo se guarda con el nombre original

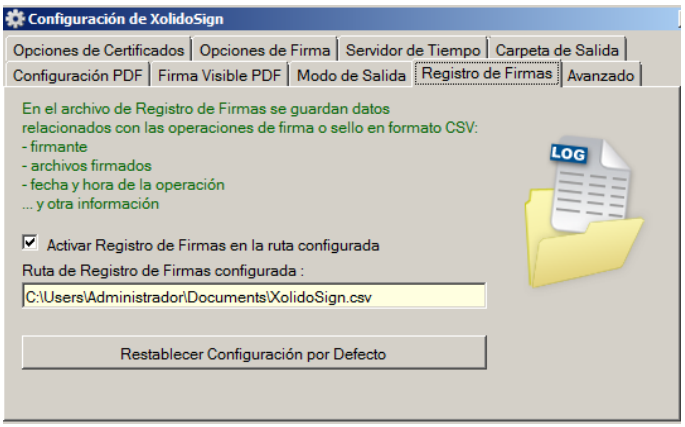
Modo por defecto: el archivo se guarda con el nombre original agregando la cadena _firmado

Modo indicativo: el archivo se guarda con el nombre original agregando la cadena _firmado_nombre básico del certificado y finalizado con la extensión original. Ejemplo: FORMATOS NUMÉRICOS PERSONALIZADOS_firmado_por_APELLIDO1_APELLIDO2.docx y el documento que contiene la firma FORMATOS NUMÉRICOS PERSONALIZADOS_firmado_por_APELLIDO1_APELLIDO2.docx.p7b

Modo carpeta: para cada firma se crea una carpeta con la fecha, hora y un identificador único para la operación de firma conjunta



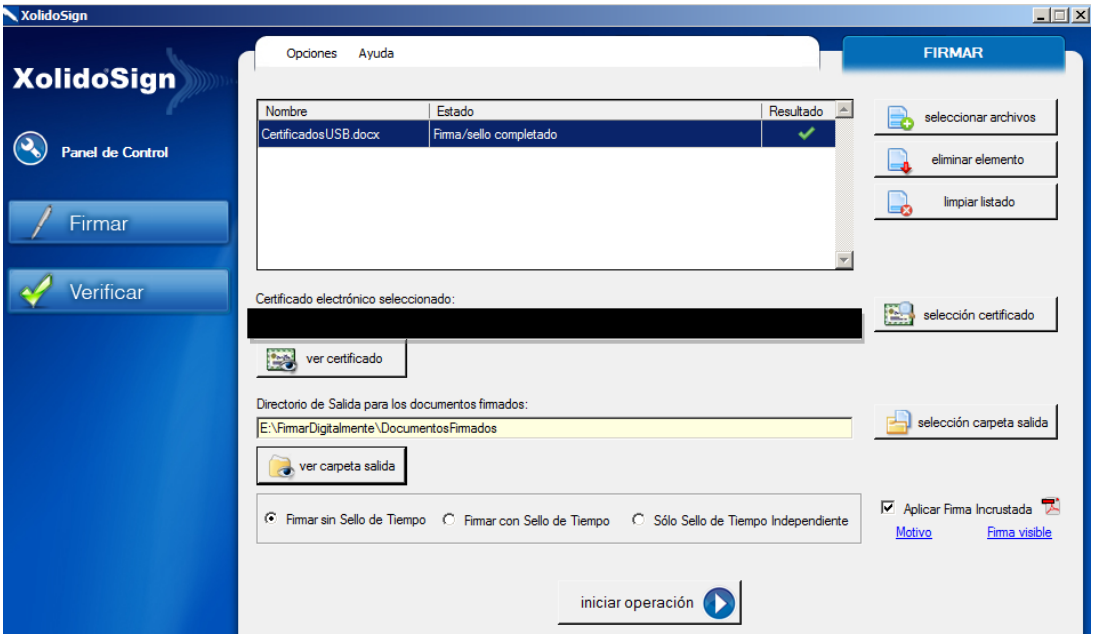
Registro de firmas



Se guardan los datos relacionados con las operaciones de firma o sellado de tiempo en formato .CSV, nombre del fichero XolidoSign.CSV

Nombre de archivo	Resumen de los datos firmados	Resultado de la operacion	Fecha y hora	Tipo de firma	Nombre del certificado	Resumen del certificado
C:\Users\Administrador\Desktop\FIRMA.pdf	DC120A7E7EB8B42A718F73A06825B969B96ED32D	OK	16/11/2010 13:30	PDF	C=ES,SERIAL NUMBER=71	[redacted]654E42
C:\Users\Administrador\Desktop\FIRMA.pdf	57B850438FB7F5CF8BD5678C85DB6F10E1CCD23B	OK	16/11/2010 13:41	PDF	C=ES,SERIAL NUMBER=71	[redacted]E42C22F
C:\Users\Administrador\Desktop\FIRMA.pdf	29C8610C48995F869DAA91A319824B01FAD59CA5	OK	16/11/2010 13:45	PDF	C=ES,SERIAL NUMBER=71	[redacted]E42C22F
E:\FirmarDigitalmente\Parafirmar\CertificadosUSB.docx	74610EF2D5295E6E90463921ECFCF7E8E5352DC8	OK	08/02/2011 12:50	PKCS7	C=ES,SERIAL NUMBER=71	[redacted]E42C22F

Para terminar volvemos a la ventana principal donde se encuentra el documento ya firmado



Al elegir la opción de modo de salida de la firma identificativo me genera un fichero con la firma con este nombre: CertificadosUSB_firmado_por_APELLIDO1_APELLIDO2.docx.p7b (nombre del fichero_firmado_por_nombre del certificado.extensión del fichero.tipo de fima)

CASOS PRÁCTICOS: FIRMAR DOCUMENTOS

[Nota: La herramienta Xolidosign, que es de libre distribución permite realizar la firma digital, no permite firmar digitalmente cada una de las páginas, puesto que lo que se firma digitalmente es todo el documento. Caso que compruebas luego desde el acrobat, por ejemplo y ves que está firmado digitalmente. De hecho no es necesario que aparezca incrustada la firma]

En el caso de los documentos de Word, la firma no se incrusta en el documento con lo que me genera el documento de Word sin la firma visible y documento con la firma

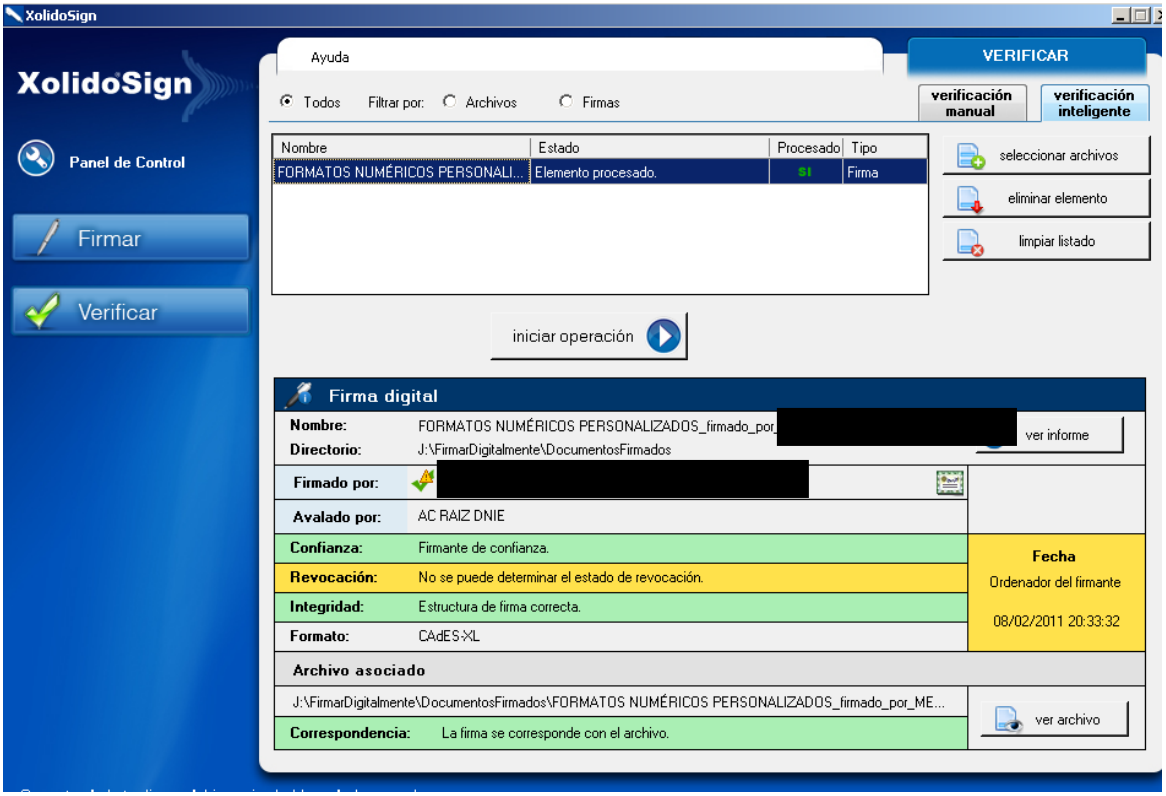
FORMATOS NUMÉRICOS PERSONALIZADOS_firmado_por_APELLIDO1_APELLIDO2.docx

FORMATOS NUMÉRICOS PERSONALIZADOS_firmado_por_APELLIDO1_APELLIDO2.docx.p7b

Sólo en los documentos PDF se puede elegir la ubicación de la firma e insertarle una imagen

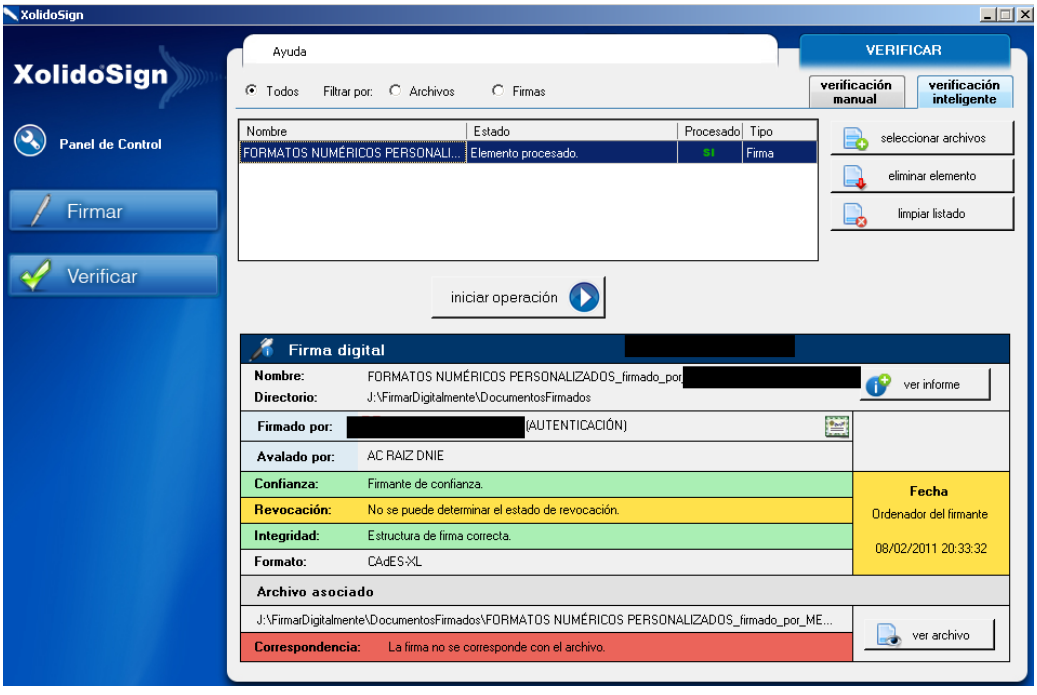
En caso que un documento que fue firmado digitalmente sea modificado lo vamos a saber al verificar la firma

Comprobamos la validez de la firma y que el documento no fue modificado (siguiente imagen):



Nos indica que la firma se corresponde con el archivo (el archivo no fue modificado)
Abrimos el .docx y añadimos algún cambio al documento y lo guardamos

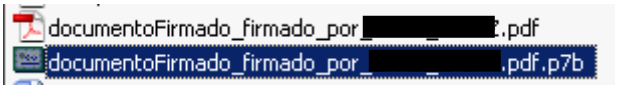
Abrimos de nuevo el archivo de firma: FORMATOS NUMÉRICOS PERSONALIZADOS_firmado_por_APELLIDO1_APELLIDO2.docx.p7b y nos indica que el documento sufrió algún cambio desde que fue firmado



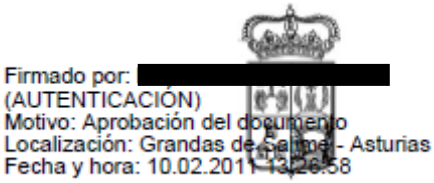
FIRMAR UN PDF

Ya tenemos configurado el Xolidosign

Ejemplo de un pdf firmado con Xolidosign aplicando la configuración anterior:



Si cambiamos las opciones de firma a "firma electrónica básica) obtenemos este resultado al firmar un pdf (mostramos la línea de firma incrustada en este caso en la parte inferior izquierda con la imagen de la entidad como fondo) al mismo tiempo que desde el panel de firma del PDF vemos las características de la firma



APLICACIÓN AUTOFIRMA

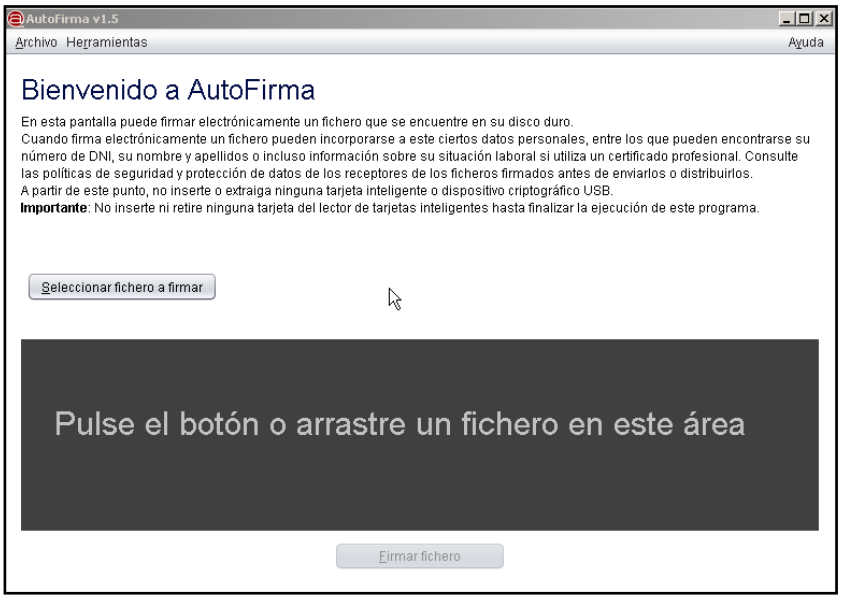
AutoFirma es una herramienta de escritorio con interfaz gráfica que permite la ejecución de operaciones de firma de ficheros locales en entornos de escritorio (Windows, Linux y Mac OS X). También puede utilizarse a través de consola o ser invocada por otras aplicaciones mediante protocolo para la ejecución de operaciones de firma

Compatible con sistema Windows 7 y versiones superiores

Distribuciones GNU/Linux indicadas en el manual de la aplicación

MAC

Interfaz gráfica de autofirma:

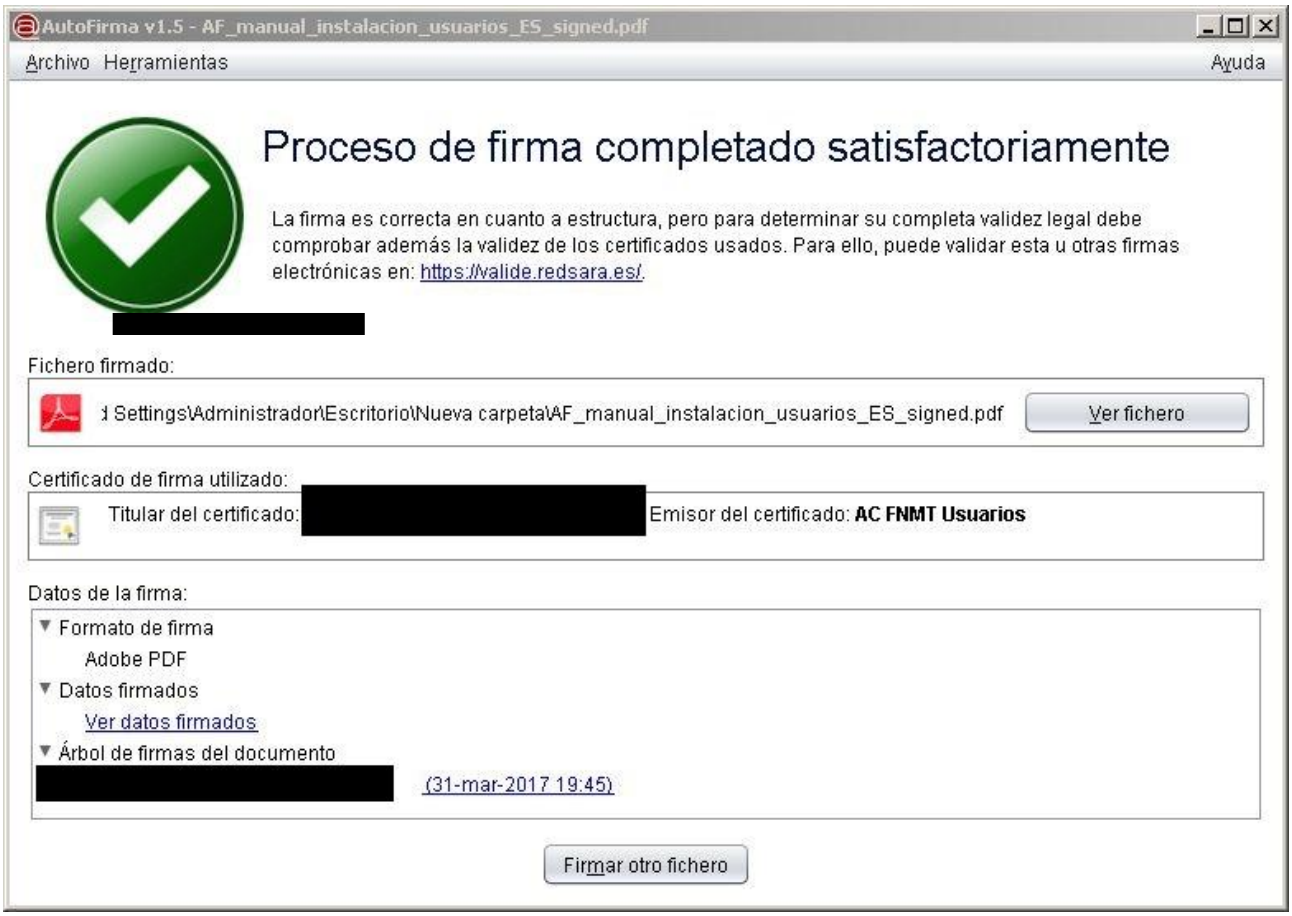


Configuramos el programa y firmamos el documento. Si necesitamos sellado de tiempo lo configuramos. Los datos del servidor de sellado nos los tiene que facilitar una autoridad certificadora

Una vez firmado el documento nos genera el fichero "AF_manual_instalacion_usuarios_ES_signed.pdf"

Usé para firmar el certificado de usuario de la FNMT

En la captura de pantalla se muestra el proceso de firma completado



VALIDAR UNA FIRMA REALIZADA y comprobar que no ha sido modificada:

VALIDE > https://valide.redsara.es/valide/inicio.html

SELLADO DE TIEMPO

(CAMERFIRMA: El time stamping o **sellado de tiempo** es el complemento ideal a la seguridad que ofrecen los certificados digitales de identidad. Mediante la aplicación del sellado de tiempo garantizamos el momento exacto en el tiempo en que la firma de un documento se produjo.)

AUTOFIRMA EN WORD

INSTALAR AUTOFIRMA

RENOVAR CERTIFICADO FNMT

APPS QUE USAN EL SISTEM NFC DEL DNI 3.0:

https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_034

(Muestra ejemplos de apps para consumir determinados servicios)

Para realizar determinados trámites con algunas administraciones es necesario instalar el programa de firma **AUTOFIRMA**