Centro de Tiflotecnología e Innovación - CTI
Camino de Hormigueras 172, Madrid 28031
T: (+34) 91 709 76 00 · F: (+34) 91 709 77 77
https://cti.once.es/

IDENTIFICACIÓN DIGITAL - 2023

Centro de Tiflotecnología e Innovación - CTI
Camino de Hormigueras 172, Madrid 28031
T: (+34) 91 709 76 00 · F: (+34) 91 709 77 77
https://cti.once.es/

INTRODUCCIÓN

La identificación digital es un conjunto de procedimientos digitales que, a través de un sistema informático desarrollado, son capaces de verificar la identidad de una persona.

La identificación digital surge desde la necesidad de asegurar la identidad de los usuarios que operan a través de internet, principalmente ante organismos de la Administración.

En España, los sistemas de identificación digital autorizados por la Administración, están recogidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que cumple las directrices del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y quedan definidos de la siguiente forma:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".
b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".
c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca.

SISTEMAS DE IDENTIFICACIÓN DIGITAL

Los diferentes organismos de la Administración, como la Agencia Tributaria o la Seguridad Social, entre los más populares, posibilitan la realización de trámites a través de sus oficinas virtuales mediante diversos sistemas de identificación digital: Certificado o DNI electrónico, Cl@ve PIN y otros sistemas de identificación, válidos para determinados servicios, como son Número de referencia, habilitada para diversos trámites de Renta y CSV (Código Seguro de Verificación), que permite el acceso a consulta de documentos electrónicos y descarga de ficheros.

Características de los Certificados Digitales

- Es un documento electrónico expedido por una Autoridad de Certificación e identifica a una persona (física o jurídica) con un par de claves.
- Tiene como misión validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta.
- Contiene la información necesaria para firmar electrónicamente e identificar a su propietario con sus datos: nombre, NIF, algoritmo y claves de firma, fecha de expiración y organismo que lo expide.
- La Autoridad de Certificación da fe de que la firma electrónica se corresponde con un usuario concreto. Esa es la razón por la que los certificados están firmados, a su vez, por la Autoridad de Certificación.

En un Certificado, las claves digitales son los elementos esenciales para la firma e identificación del firmante. Existen dos claves, la clave privada y clave pública, y trabajan de forma complementaria. Lo que cifra o codifica una clave sólo lo puede descifrar o decodificar la otra.

La diferencia entre ellas es que la clave privada está pensada para que nunca salga del certificado y esté siempre bajo el control del firmante. En cambio, la clave pública se puede repartir o enviar a otros usuarios.

En ocasiones, se habla de Certificado Privado para referirse al certificado que contiene la clave privada y la pública, y del Certificado Público para referirse al certificado que sólo contiene la clave pública.

Para obtener el Certificado Digital hay que tener en cuenta si el certificado está destinado a ser incluido en una tarjeta, como el DNIe, o si el certificado se guarda en un fichero software.

En ambos procesos es necesario identificar al responsable o usuario del certificado, para lo cual se requiere que éste se persone en las oficinas de una Autoridad de Registro, donde corroborarán su identidad.

En el caso de los certificados software, el propio navegador del usuario crea las claves. Pero, en el Certificado de tarjeta, quien crea e introduce las claves es el Proveedor de Certificación.

Por otra parte, los certificados contenidos en tarjetas (DNIe) deben ser entregados directamente al usuario, y para ello debe personarse en las oficinas de la Dirección General de Policía, que es la Autoridad Certificadora.

Los Certificados electrónicos tienen un periodo de validez pasado el cual no sirven para firmar ni tampoco para identificarse.

Cada Proveedor de Certificación establece unos plazos antes de que el certificado caduque para poder renovarlo sin necesidad de otra identificación. En el caso de los certificados de la FNMT, tienen una validez de 36 meses y se puede renovar durante los 2 meses anteriores a su caducidad.

Los Certificados incluidos en la tarjeta de DNIe tienen una validez de 30 meses (aunque la tarjeta del DNIe puede tener una validez de hasta 10 años dependiendo de la edad de la persona). Si el Certificado caduca hay que volver a realizar todo el proceso de solicitud del certificado, aunque se puede renovar antes de que caduque y, entonces, el proceso no requiere una solicitud nueva.

En el caso de disponer de DNIe con certificados en vigor, no será necesario personarse en las oficinas de registro para obtener el certificado digital.

Centro de Tiflotecnología e Innovación - CTI
Camino de Hormigueras 172, Madrid 28031
T: (+34) 91 709 76 00 · F: (+34) 91 709 77 77
https://cti.once.es/

CERTIFICADO DIGITAL

El Certificado Digital FNMT de Persona Física es la certificación electrónica expedida por la FNMT-RCM que vincula a su suscriptor con unos datos de verificación de firma y confirma su identidad.

Este certificado, también conocido como Certificado de Ciudadano o de Usuario, es un documento digital que contiene sus datos identificativos. Le permitirá identificarse en Internet e intercambiar información con otras personas y organismos con la garantía de que sólo Ud. y su interlocutor pueden acceder a ella.

Quién puede obtener el Certificado Digital

Cualquier ciudadano español o extranjero, mayor de edad o menor emancipado que esté en posesión de su DNI o NIE, podrá solicitar y obtener su certificado digital de forma gratuita para firmar y acreditar su identidad de forma segura en Internet.

Para qué sirve

El Certificado Digital de Persona Física le permitirá realizar trámites de forma segura con la Administración Pública y entidades privadas a través de Internet, como por ejemplo:

- Presentación y liquidación de impuestos
- Presentación de recursos y reclamaciones
- Cumplimentación de los datos del censo de población y viviendas
- Consulta e inscripción en el padrón municipal
- Consulta de multas de circulación
- Consulta y trámites para solicitud de subvenciones
- Consulta de asignación de colegios electorales
- Actuaciones comunicadas
- Firma electrónica de documentos y formularios oficiales

Gracias a su Certificado FNMT de Persona Física podrá olvidarse de desplazamientos y esperas innecesarias.

Obtención e instalación del Certificado Digital

Actualmente existen cuatro formas de obtener el Certificado Digital:

- Mediante DNI electrónico. Si se dispone de un DNI electrónico con certificados en vigor, se puede solicitar el certificado digital sin necesidad de desplazarse a las oficinas de registro a través de un lector de DNI electrónico. En el caso de que los certificados del DNI electrónico hayan caducado, existe la posibilidad de acudir a una Comisaría de Policía para renovarlos a través de las máquinas destinadas a tal efecto. Dichas máquinas disponen de entrada de auriculares para que las personas ciegas puedan realizar el proceso de forma autónoma.
- Utilizando un dispositivo móvil. Para realizar este proceso hay que descargar la App Certificado Digital FNMT desde el App Store o Google Play, dependiendo del tipo de dispositivo a utilizar y, a continuación, acreditar la identidad mediante vídeo identificación desde el propio móvil, o de forma presencial en una oficina de registro. Tras acreditar la identidad, ya es posible descargar el Certificado.

- Con vídeo identificación. Tras la obtención del código de solicitud en la web de la FNMT, se puede acreditar la identidad mediante vídeo identificación, petición que suele ser atendida en un plazo máximo de 2 días y cuya aprobación se notifica mediante correo electrónico. Tras realizar este proceso, para el que se utiliza una webcam, se podrá descargar el Certificado obtenido.
- Personándose en alguna de las oficinas de registro para identificarse. En el caso de que no se disponga de DNI electrónico con certificados en vigor, será necesario solicitar el certificado en alguna de las oficinas de registro. Dichas oficinas suelen ser las de la Seguridad Social y las de la Agencia Tributaria.

El procedimiento para solicitar el certificado en una de estas oficinas es el siguiente:

En primer lugar hay que acceder a la web de la FNMT (Solicitar Certificado - Sede (fnmt.gob.es) y descargar el configurador FNMT, que es la herramienta que va a permitir generar el documento necesario para identificarse en las oficinas de registro.

Una vez hecho esto, deberá rellenarse el formulario con los datos requeridos (DNI, primer apellido y dirección de correo electrónico).

Al rellenar estos datos, se abrirá el configurador FNMT, donde se introducirá una contraseña para proteger la solicitud. Dicha contraseña deberá recordarse posteriormente para descargar el certificado o para hacer una copia de seguridad del mismo.

NOTA: Es importante tener en cuenta que, para los usuarios de Jaws, será necesario tener instalado Java Access Bridge. Esta funcionalidad ya viene incluida en las últimas versiones de Java, pero, para que funcione correctamente con Jaws, es importante asegurarse de que la versión que está instalada en el ordenador sea de 64 bits. Esta versión se encuentra disponible para su descarga en la web de Java.

Una vez creada la contraseña y después de pulsar el botón “aceptar”, se recibirá un correo de la FNMT con un código. Este código es el que se deberá aportar en la oficina de registro para identificarse. A continuación, se recibirá una notificación para la descarga del certificado digital en la misma cuenta de correo electrónico que se utilizó para hacer la solicitud.

Al acceder al enlace para descargar el certificado, se volverá a abrir el configurador FNMT, donde habrá que introducir la contraseña utilizada en la solicitud. Tras introducir la contraseña, es posible hacer una copia de seguridad del certificado. En caso de ser así, hay que especificar la ruta donde se quiere guardar dicha copia. Una vez finalizada la copia, el certificado quedará instalado en todos los navegadores del equipo.

NOTA: hay que tener en cuenta que todo el proceso de solicitud y de instalación del certificado debe hacerse desde el mismo ordenador y con el mismo perfil de usuario.

Importar y exportar el Certificado Digital

Una vez obtenido el certificado, durante el proceso de instalación, se puede crear un archivo para poder utilizarlo en distintos ordenadores. En el caso de que no se haya guardado durante el proceso de instalación, existe la posibilidad de hacerlo posteriormente.

Dependiendo del navegador que se utilice, la forma de acceder a la opción puede variar, pero el procedimiento es similar en todos los casos.

A continuación, se explicarán los pasos a seguir para exportar el certificado dependiendo del navegador que se tenga instalado.

• **Microsoft** Edge

En Microsoft Edge se deberá acceder a la opción “configuración y más”, entrar en “configuración”, buscar la opción “privacidad, búsqueda y servicios” y acceder al apartado de “seguridad” donde se encuentra un botón para administrar los certificados.

Al pulsar el botón "Exportar", aparecerá un asistente que guiará al usuario en el proceso de exportación del certificado.

Se seleccionará la opción "Exportar la clave privada" y se pulsa "Siguiente".

En "Formato de archivo de exportación" dejar las opciones tal y como se muestran por defecto y pulsar "Siguiente".

Se llegará a una pantalla donde se introducirá una contraseña y se confirmará para proteger el archivo que contiene el certificado exportado. Esta misma contraseña se utilizará para importar el certificado desde otro navegador o equipo, así que es muy importante no olvidarla. A continuación, se pulsará el botón "Siguiente".

En el siguiente cuadro de diálogo, se debe indicar la ruta y el nombre del archivo correspondientes al certificado exportado, para ello se pulsará el botón "Examinar", una vez elegida la ruta y el nombre del archivo pulsar "Guardar", y, para finalizar, pulsar el botón "Siguiente".

• **Mozilla Firefox**

Abrir el almacén de certificados del navegador Mozilla Firefox:

Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados - botón Ver certificados, pestaña de "Sus Certificados".

Seleccionar el certificado y pulsar "Hacer copia".

Indicar dónde se quiere realizar la copia de seguridad (disco duro, cd, unidad de red, etc.).

Introducir la contraseña maestra del navegador (si se estableció).

Introducir una contraseña y confirmarla para proteger la copia de seguridad que se va a realizar y pulsar “Aceptar”.

Si el proceso es correcto, se habrá creado un nuevo fichero en la ruta seleccionada con extensión *.p12.

• **Google Chrome**

Google Chrome en Windows utiliza el almacén de certificados de Internet Explorer.

Para exportar un certificado con Google Chrome debe dirigirse a "Personalizar y Configurar Google Chrome" / Configuración.

En Opciones Avanzadas / HTPPS/SSL pulsar "Administrar certificados". Seleccionar el que se quiere exportar y pulsar el botón "Exportar". A partir de este momento seguir el asistente de Windows.

Se puede elegir entre exportar la clave privada o no, dependiendo del uso que se quiera hacer del certificado.

Exportación del certificados con clave privada

Dejar las opciones tal y como se muestran por defecto y pulsar "Siguiente". Se accederá a una pantalla donde se pide una contraseña y su validación para proteger el archivo.

En el siguiente cuadro de diálogo indicar la ruta y el nombre del archivo que se quiere que contenga el certificado exportado, pulsar el botón "Siguiente".

A continuación, se muestra una ventana con las características del certificado exportado, pulsar el botón "Finalizar" y aparecerá un mensaje de aviso diciendo que la clave privada va a ser exportada, pulsar "Aceptar" y si la operación ha sido correcta se mostrará un cuadro informando de que el certificado ha sido exportado con éxito.

Exportación de certificados con clave pública, pero sin clave privada

Seleccionar la opción de No exportar la clave privada y pulsar "Siguiente" Marcar la opción "DER binario codificado X.509 (.CER)" y pulsar "Siguiente" Introducir la ruta y el nombre del archivo que contendrá el certificado exportado.

A continuación, se muestra una pantalla con las propiedades del certificado exportado, pulsar "Finalizar" y si la operación se ha realizado correctamente aparecerá un mensaje confirmando la exportación correcta del certificado

Llavero de MAC

Para exportar el certificado personal desde el llavero de MAC, deberá hacerse lo siguiente:

Abrir la utilidad de llaveros, para ello pulsar en Ir / Utilidades / Acceso a llaveros.

Pulsar en Mis Certificados y seleccionar el certificado que se desea exportar.

Pulsar en Archivo - Exportar elementos.

Elegir un nombre de archivo y la ruta donde se guardará.

Introducir la contraseña y confirmarla. Pulsar OK.

El certificado será guardado con extensión .p12.

iPhone

Para guardar el certificado en un iPhone se seguirán los siguientes pasos:

Descargar el certificado en los archivos del iPhone. Una vez que se cuente con el certificado, será suficiente con abrir el archivo que lo contiene.

Si aparece un mensaje preguntando dónde se quiere instalar el certificado se seleccionará iPhone.

Ante el aviso de “Perfil descargado”, tocar sobre “cerrar”.

Abrir la App ajustes en el iPhone.

En la parte superior, bajo nuestro nombre, tocar en “Perfil descargado”.

Tocar “Instalar”.

Introducir la contraseña del iPhone.

Si aparece un aviso afirmando que “El perfil no está firmado”, tocar en ”Instalar” y confirmar tocando de nuevo “Instalar”.

Introducir la contraseña del certificado.

Tocar “Siguiente”.

Pulsar OK.

Android

El proceso de instalación es muy parecido a ejecutar un archivo Apk, solo se necesita pulsar sobre el certificado digital para que Android lo instale. El proceso se realiza de la siguiente manera:

Mover el archivo original del certificado al teléfono y sin comprimir. Esto se puede hacer enviándolo como adjunto en un correo electrónico y, desde allí, guardarlo en el teléfono, por ejemplo.

Guardar el certificado digital en el almacenamiento del móvil.

Abrir el administrador de archivos del móvil y buscar la ruta donde se guardó el archivo que contiene el certificado.

Pulsar sobre el archivo para abrirlo y escribir la clave con la que se cifró.

Importar certificado

A continuación, se explicará el proceso de importación del certificado dependiendo del navegador que se tenga instalado.

• Microsoft Edge

En Microsoft Edge hay que acceder a la opción “Configuración y más”, entrar en “Configuración”, buscar la opción “Privacidad, búsqueda y servicios” y acceder al apartado de “Seguridad”, donde se encuentra un botón para administrar los certificados.

Pulsar el botón "Importar" para iniciar el asistente que llevará a cabo el proceso de importación del certificado. A continuación, pulsar "Siguiente", y en “Examinar”, seleccionar la ruta y el nombre del fichero del certificado que se quiere importar. A continuación, pulsar "Siguiente".

En la nueva ventana, introducir la contraseña con la que está protegido el fichero y marcar las dos casillas: "Habilitar protección segura de clave privada..." y "Marcar la clave privada

como exportable..." para volver a exportar el certificado con la clave privada. Pulsar "Siguiente".

A continuación, se indica donde se puede colocar el certificado importado, se deja la opción por defecto y pulsar "Siguiente" y "Finalizar". Para asignar una contraseña al certificado, pulsar "Nivel de seguridad", establecerlo en “Alto” y escribir la contraseña dos veces. Para terminar, pulsar “Finalizar”, y volver a introducir la contraseña definida y cerrar el asistente.

Si todo el proceso se realiza de forma adecuada, aparecerá un mensaje informando de que el certificado ha sido importado correctamente.

• Mozilla Firefox

NOTA: para importar un certificado al almacén de Firefox correctamente, la copia de seguridad debe tener contraseña asignada, esto es, que cuando se exportó se le asignó dicha contraseña y no se dejó en blanco.

Ir al almacén de certificados del navegador Mozilla Firefox:

Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados - botón “Ver certificados”, pestaña "Sus Certificados".

Pulsar en el botón "Importar".

Buscar la ubicación (disco duro, cd, memoria USB, unidad de red) de la copia del certificado que se quiera importar.

Introducir la contraseña maestra de su navegador (si se estableció alguna). Si es la primera vez que se usa este navegador con certificados, introducir y confirmar una contraseña. Esta contraseña tendrá que ser utilizada cada vez que se use el certificado en las webs que lo requieran.

Introducir la contraseña con la que se protegió la copia de seguridad.

Comprobar que la copia de seguridad se ha realizado.

• Google Chrome

Google Chrome en Windows utiliza el almacén de certificados de Internet Explorer.

Para importar un certificado con Google Chrome, ir a Personalizar y Configurar Google Chrome / Configuración.

En Opciones Avanzadas / HTPPS/SSL, pulsar "Administrar certificados".

A continuación, pulsar el botón "Importar" y aparecerá un asistente que guiará al usuario durante el proceso de importación del certificado. Pulsar "Siguiente" e introducir en el cuadro de diálogo el nombre del fichero que tiene el certificado a importar y pulsar "Siguiente".

En la siguiente ventana se pide la contraseña con la que está protegido el fichero, introducirla y marcar la casilla "Marcar la clave privada como exportable" para permitir volver a exportar el certificado con la clave privada. Pulsar "Siguiente".

A continuación, se sugiere la ubicación del certificado importado. Mantener dicha opción y pulsar "Siguiente".

En la siguiente ventana se muestra un cuadro con las propiedades del certificado importado, pulsar Aceptar y, si el proceso se ha completado con éxito, aparecerá un mensaje informando de que el certificado ha sido importado correctamente.

• Llavero de MAC

Para importar el certificado personal al llavero de MAC se debe hacer lo siguiente:

Abrir la utilidad de llaveros con Ir / Utilidades / Acceso a llaveros.

Pulsar en Llaveros, Inicio de sesión y marcar la categoría “Mis Certificados”.

A continuación, pulsar Archivo - Importar ítems.

Seleccionar el archivo de copia de seguridad (.pfx o .p12) y pulsar Abrir.

Introducir la contraseña y pulsar OK.

Cómo utilizar el Certificado

Una vez realizado el proceso de instalación, al acceder a la Sede Electrónica del organismo en el que se desee realizar determinados trámites, será necesario identificarse a través del certificado.

El proceso de identificación es sencillo, ya que cuando llegue el momento de hacerlo, aparecerá una ventana en la que se mostrarán los certificados instalados. En esta ventana, basta con seleccionar el certificado a utilizar y la identificación se habrá completado. A continuación, podrá realizarse el trámite deseado.

DNI ELECTRÓNICO

El DNI electrónico es un documento emitido por la Dirección General de la Policía (Ministerio del Interior). Además de acreditar físicamente la identidad personal de su titular permite:

- Acreditar electrónicamente y de forma inequívoca su identidad.
- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita.

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

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

Certificados Electrónicos en el DNIe
Con el DNI electrónico se obtienen dos certificados:

- Certificado de Autenticación: Garantiza electrónicamente la identidad del ciudadano al realizar una transacción telemática. Este Certificado asegura que la comunicación electrónica se realiza con la persona que dice ser, con el certificado de identidad y la clave privada asociada al mismo.
- Certificado de Firma: Permite la firma de trámites o documentos, sustituyendo a la firma manuscrita. Por tanto, garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma.

Obtención del DNIe

Para obtener el DNIe se deberá acudir a una Oficina de Expedición del DNI electrónico, abonar la tasa establecida y presentar los siguientes documentos:

- Certificación literal de nacimiento expedida por el Registro Civil correspondiente.
- Una fotografía reciente.
- Certificado o volante de empadronamiento del Ayuntamiento.

Los españoles residentes en el extranjero acreditarán el domicilio mediante certificación de la Representación Diplomática o Consular donde estén inscritos como residentes.

Cambiar el PIN

En el momento de la expedición, se genera un PIN aleatorio que se entrega en forma de 'sobre ciego'. Se puede cambiar este PIN en cualquier momento en los Puntos de Actualización del DNI electrónico (PAD) ubicados en las Oficinas de Expedición.

Si el DNI está bloqueado o no se recuerda el PIN, se podrá usar la huella dactilar, que también está almacenada en el DNI, para desbloquearlo.

Cómo utilizar el DNIe

Requisitos Técnicos

Para la utilización del DNIe, es necesario contar con determinados elementos hardware y software que permitirán el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

Mientras que el DNIe sólo permite el acceso mediante contacto, el DNI 3.0 dispone de un chip Dual interface, que permite también la conexión inalámbrica a través de la antena NFC.

Para la utilización mediante contacto se necesita:

- Un ordenador personal.
- Un lector de tarjetas inteligentes. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una tarjeta PCMCIA.

Para la utilización sin contacto se necesita 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. Éste dispositivo puede ser un Smartphone, una tablet o un lector NFC.

En cuanto a software, el DNI electrónico es compatible con los sistemas operativos actualmente existentes, así como con los distintos navegadores.

El procedimiento de identificación con el DNIe precisa que éste se encuentre insertado en el lector, y este último a su vez, conectado al ordenador. En el momento de acceder al trámite elegido, el navegador detectará automáticamente el certificado del DNIe que habrá que seleccionar.

Renovación del DNIe y de los Certificados

Renovación del DNIe. La renovación se llevará a cabo mediante la presencia física del titular, que deberá abonar la tasa y aportar los documentos correspondientes. El DNI se deberá renovar dentro de los últimos 90 días de vigencia.

Renovación de los certificados. Los certificados se pueden renovar en un periodo de tiempo que abarca desde 30 días antes de la fecha de caducidad de los certificados hasta la caducidad del soporte físico (Tarjeta DNIe).

Para renovar el DNIe: Según la Ley 59/2003 de Firma Electrónica si han pasado más de 5 años desde la primera identificación, la renovación, a través de los Puntos de Actualización del DNIe, requerirán la personación previa del ciudadano ante un funcionario de la Oficina de Expedición.

La validez de los certificados contenidos en el chip de la tarjeta del DNI electrónico es de 30 meses. (Artículo 12. Validez de los certificados electrónicos, RD 1553/2005, de 23 de diciembre).

Denuncia y revocación de los Certificados

En caso de pérdida o sustracción del DNIe es obligatorio personarse en una Oficina de Expedición del DNI para denunciar su pérdida.

La revocación de los certificados electrónicos del DNIe se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida.

LA APP Cl@ve

La APP Cl@ve permite al ciudadano autenticarse en el trámite que esté realizando confirmando la petición a través de Cl@ve Móvil o recibiendo el PIN de Cl@ve PIN que solicite para acceder a una gestión.

La APP Cl@ve aúna en un solo sitio la posibilidad de identificarse electrónicamente para autenticarse en un trámite, ya sea a través de Cl@ve Móvil o Cl@ve PIN en las relaciones con las Administraciones Públicas.

Para hacer uso de los servicios de la APP Cl@ve es necesario estar registrado en el sistema Cl@ve.

La aplicación está disponible para su descarga en Google Play y Huawei AppGallery compatible con sistema operativo Android, y en Apple Store, para sistema operativo iOS.

Cl@ve Móvil

Cl@ve Móvil es el nuevo sistema de acceso electrónico a los servicios públicos que permite al ciudadano autenticarse en el trámite que esté realizando, simplemente confirmando la petición de autenticación que le llegará a la aplicación móvil Cl@ve.

Para hacer uso de los servicios de esta aplicación móvil es necesario estar registrado en el sistema Cl@ve.

Es un sistema sencillo, con el que el usuario no tiene que recordar ninguna contraseña y solo con un clic, pulsando en el aviso que le llega al dispositivo móvil (notificación push) o abriendo la APP Cl@ve, confirma la petición de autenticación, tras lo que se le redirigirá al trámite donde estaba intentando acceder.

Uso de Cl@ve Móvil

Una vez registrado en el sistema Cl@ve, para realizar una gestión de la administración electrónica, Cl@ve Móvil permitirá la autenticación en el proceso simplemente confirmando la petición que llegará a la APP Cl@ve:

- Tras acceder a la gestión, se redirigirá a la plataforma Cl@ve.
- Seleccionar Cl@ve Móvil para identificarse.
- Se redirigirá al proveedor de identidad, donde se mostrará un código QR para escanear desde la APP Cl@ve. También se puede seleccionar la opción de introducir DNI/NIE y fecha de validez del DNI (o fecha de expedición si es un DNI permanente) o número de soporte del NIE.
- Abrir la App Cl@ve para escanear el código QR o si se ha introducido DNI/NIE, pulsar en el aviso o abrir la App para visualizar la petición de autenticación con Cl@ve Móvil.
- Por seguridad, es necesario comprobar que el Organismo y el código de verificación que se muestran en la APP son los mismos que aparecen donde se está intentando acceder. Una vez confirmada la petición de Cl@ve Móvil en la App con el factor de autenticación (desbloqueo) que esté configurado en el dispositivo móvil (patrón, huella, etc.), se redirigirá automáticamente al trámite que se desee realizar.

Es necesario tener en cuenta de que sólo es posible tener activo un dispositivo para cada DNI/NIE.

Cl@ve PIN

Es una forma de realizar trámites por Internet con una validez limitada en el tiempo y que se puede renovar cada vez que se necesite. Este sistema de identificación electrónica está basado en el uso de un código elegido por el usuario y un PIN comunicado al teléfono mediante la app Cl@ve PIN o con un mensaje SMS.

Es obligatorio registrarse previamente en el sistema.

Ventajas que ofrece:

- Es muy sencillo, no es necesario recordar una contraseña de forma permanente
- Su validez es limitada en el tiempo, lo que hace que sea más seguro.

Cómo registrarse en Cl@ve PIN

Las formas de registrarse en Cl@ve PIN son las siguientes:

- Registro en Cl@ve por Internet con carta de invitación y CSV o con videollamada (nivel básico).

- Registro por Internet en el sistema Cl@ve con certificado o DNI electrónico (nivel avanzado).
- Registro presencial en el sistema Cl@ve (nivel avanzado).

Para realizar cualquiera de estos registros se debe acceder a la Sede Electrónica de la Agencia Tributaria, y, tras introducir el documento de identificación, seleccionar el tipo de registro que se desee entre los mencionados arriba.

Obtención de Cl@ve PIN
Una vez registrados hay que obtener una Cl@ve PIN para acceder a los trámites.

Por seguridad, el PIN que se recibe sólo puede ser utilizado una vez.

Se puede obtener el PIN de dos formas, aunque se recomienda utilizar la aplicación Cl@ve PIN para dispositivos móviles:

- Aplicación móvil Cl@ve PIN
- Recibir el PIN mediante SMS

El PIN que se recibe se debe utilizar para completar el acceso al sistema antes de 10 minutos. Pasado ese tiempo, si no se ha accedido a Cl@ve, se deberá solicitar un nuevo PIN.

Una vez identificado mediante el PIN, se puede acceder a los servicios que permita Cl@ve hasta desconectarse de la Sede Electrónica o cerrar el navegador.

Cómo usar Cl@ve PIN
Una vez que se ha obtenido un PIN, se selecciona el trámite que se desea realizar y se cumplimenta:

- DNI/NIE
- Clave de acceso, que está formada por el código elegido cuando se solicitó y los tres caracteres del PIN recibido en el teléfono móvil.

NOTA: el código de acceso sólo puede ser utilizado una vez.

Una vez identificado mediante el PIN se puede acceder a los servicios que permita Cl@ve hasta desconectarse de la Sede Electrónica o cerrar el navegador.

Cl@ve permanente
Es un sistema de autenticación diseñado para personas que necesitan acceder frecuentemente a los servicios electrónicos de la Administración. Se basa en el uso de un código de usuario, su DNI o NIE, y de una contraseña que se establece en el proceso de activación y que sólo debe ser conocida por uno mismo. Para acceder al proceso de activación es necesario haberse registrado previamente en el sistema.

Para los servicios de administración electrónica que requieran un nivel de seguridad elevado, el sistema refuerza la autenticación con la solicitud de introducción de un código numérico de un solo uso (One Time Password, OTP) que se envía previamente por mensaje SMS al teléfono móvil.

Centro de Tiflotecnología e Innovación - CTI
Camino de Hormigueras 172, Madrid 28031
T: (+34) 91 709 76 00 · F: (+34) 91 709 77 77
https://cti.once.es/

Cómo funciona

Una vez se haya seleccionado Cl@ve Permanente como modo de acceso para acceder al servicio de administración electrónica, el sistema presentará la siguiente pantalla:

Si la contraseña introducida es correcta, y el servicio no requiere un nivel de seguridad más elevado, se permitirá el acceso al mismo.

Si, por el contrario, el servicio al que se quiere acceder requiere mayor nivel de seguridad, se solicitará la introducción de un código numérico de un solo uso (OTP), que previamente se remitirá vía SMS al número de móvil que se facilitó en el acto de registro.

Procedimientos

A continuación, se describen los procedimientos relacionados con la activación, uso y gestión personal de Cl@ve Permanente.

Activación de usuario

Mediante este servicio se puede activar el usuario de Cl@ve Permanente y crear una contraseña de acceso.

Para la activación del usuario de Cl@ve Permanente se debe acceder al servicio de activación donde se introducirá el usuario (DNI o NIE), la dirección de correo electrónico (como dato adicional de contraste) y el código de activación que se suministró en el acto de registro.

Si los datos son correctos, el sistema enviará un SMS con un código numérico de un solo uso (One Time Password, OTP) que se deberá teclear en el campo del formulario correspondiente. Si es correcto, el sistema permitirá establecer la contraseña que se prefiera, siempre que cumpla con unas características mínimas de seguridad. Esta contraseña será la que se deberá utilizar de ahora en adelante cada vez que un servicio de administración electrónica la solicite.

Si el código de activación se introduce erróneamente más de 5 veces, el sistema informará de ello y acto seguido bloqueará el código de activación. En este caso será necesario generar un nuevo código, para lo cual deberá repetirse el proceso de registro en Cl@ve.

Gestión de la contraseña

Si se ha olvidado la contraseña o simplemente se desea cambiar, es posible volver a establecerla de nuevo en cualquier momento con uno de los siguientes procedimientos:

Cambio de Contraseña

Por motivos de caducidad o seguridad, se puede desear cambiar la contraseña. Para ello será necesario acceder al servicio de cambio de contraseña y seguir los pasos que allí se describen.

Olvido de Contraseña

En caso de olvido de la contraseña o de que ésta quede bloqueada por superarse el número máximo de 5 intentos fallidos, se podrá establecer una nueva contraseña siempre que se haya conservado el código de activación. Para ello se deberá acceder al servicio de activación de contraseña y seguir los pasos allí indicados.

Pérdida del Código de activación

Si no se ha conservado el código de activación, se puede obtener uno nuevo realizando de nuevo el acto de registro en Cl@ve.

Regenerar el Código de Activación de Cl@ve permanente

Si ya se está registrado en Cl@ve y se necesita, puede regenerarse el Código de Activación de Cl@ve permanente.

Baja de usuario

Es posible dar de baja el usuario de Cl@ve Permanente utilizando este servicio.

Si por cualquier causa no se desea mantener activo el usuario de Cl@ve Permanente, se deberá hacer uso del servicio de baja, al que se podrá acceder con Cl@ve Permanente actual o con certificado digital.

Si se accede mediante Cl@ve Permanente, una vez introducida ésta, el sistema enviará un SMS con un código numérico de verificación que se deberá teclear en el campo del formulario correspondiente y, si es correcto, el sistema dará de baja el usuario de Cl@ve Permanente.

Si se ha olvidado la contraseña y desea darse de baja, se puede acceder con certificado digital. En este caso no se solicitará el código de verificación y la baja se realizará de manera inmediata.

Si en algún momento posterior se desea volver a activar Cl@ve Permanente, deberá realizarse de nuevo el trámite de registro en Cl@ve.

Centro de Tiflotecnología e Innovación - CTI
Camino de Hormigueras 172, Madrid 28031
T: (+34) 91 709 76 00 · F: (+34) 91 709 77 77
https://cti.once.es/

Cl@ve Firma

Cl@ve es un sistema de Identificación, Autenticación y Firma Electrónica para los ciudadanos común a todo el Sector Público Administrativo Estatal, basado en el uso de claves concertadas, conforme a lo previsto en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y conforme al Reglamento Europeo de Identidad y Firma Electrónica 910/2014.

La principal novedad que incorpora el sistema Cl@ve es la posibilidad de realizar firma electrónica mediante certificados electrónicos centralizados, es decir, certificados electrónicos almacenados y custodiados por la Administración Pública.

Estos certificados centralizados, o "certificados en la nube" permiten al ciudadano firmar documentos electrónicos desde cualquier dispositivo que tenga conexión a Internet y sin ningún equipamiento adicional.

Para utilizar la firma centralizada es necesario haber realizado previamente los siguientes pasos:

Registro de Nivel Avanzado en el sistema Cl@ve: el ciudadano proporciona sus datos de registro en el sistema, bien de forma presencial en una oficina ante un empleado público habilitado al efecto, o bien de forma telemática, previa autenticación del ciudadano mediante un certificado electrónico reconocido.

Activación de la Cl@ve Permanente; obtención de credenciales de acceso al sistema mediante identificador de usuario y contraseña, que debe ser custodiada por el ciudadano. La validez de la contraseña está limitada en el tiempo. Adicionalmente, y cuando el tipo de trámite lo requiera, la modalidad de identificación Cl@ve permanente podrá proporcionar un nivel de garantía en la autenticación superior, mediante una verificación de seguridad adicional a través de un código de un solo uso (OTP, “One Time Password”) que se envía al dispositivo móvil del usuario. Los requisitos de seguridad de las contraseñas para este sistema se publicarán en el portal Cl@ve(http://www.clave.gob.es)

Generación del certificado de firma. Esta acción se puede realizar de manera automática en el momento de realizar la primera firma, o en cualquier otro momento a voluntad del usuario.

Los certificados necesarios para poder realizar firma centralizada, son emitidos y custodiados por la Dirección General de la Policía. Dicha custodia se realiza de manera segura, de tal forma que sólo el propietario del certificado puede tener acceso a los mismos. La Gerencia de Informática de la Seguridad Social (GISS), se constituye en Prestador de Servicios de Confianza, junto con la DGP que, además, es Autoridad de Firma. La GIS queda encargada de la custodia de una copia de seguridad de los certificados con el mismo nivel de seguridad que el fichero original.

La expedición del Certificado irá asociada al soporte físico del documento que haya sido utilizado para el registro en Cl@ve y que será, en el caso de ciudadanos españoles, el Documento Nacional de Identidad, en el caso de extranjeros comunitarios, el Certificado de Registro de Ciudadano de la Unión acompañado del Pasaporte o documento de identificación del país del interesado, y en el caso de ciudadanos extranjeros, la Tarjeta de

Extranjero. La caducidad de estos documentos llevará aparejada la caducidad de los certificados asociados a los mismos.

El duplicado de los documentos de identificación a los que hace mención el presente documento, por los motivos de deterioro, pérdida o sustracción no llevará aparejada necesariamente la revocación de los certificados centralizados, pudiendo mantenerse los ya emitidos con el documento original.

El proceso de firma se realiza con el nivel más alto de seguridad, lo que implica que se utilizará la modalidad reforzada de Cl@ve permanente, es decir, aquella en la que, además de introducir el usuario y la contraseña o Cl@ve permanente, se deberá proporcionar también la contraseña de un solo uso que se recibirá mediante un SMS enviado al teléfono asociado al titular del certificado en el momento del registro.

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:

- Identificar al firmante de manera inequívoca.
- 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.
- Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos 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.

El Certificado Electrónico, base de la firma electrónica

Para firmar un documento es necesario disponer de un certificado digital o de un DNI electrónico.

El certificado electrónico o el DNI electrónico contiene 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 de Firma Electrónica

El proceso básico que se sigue para la firma electrónica es el siguiente:

- El usuario dispone de un documento electrónico (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.
- La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
- La aplicación utiliza la clave privada 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.

Cómo firmar un documento

Algunas de las preguntas que pueden surgir en el proceso anterior son:

- ¿Qué herramienta se debe utilizar para firmar?
- ¿Es necesario instalar algo en el ordenador?
- Y cuando se firma un formulario en Internet, ¿se debe instalar algo o el navegador ya lo hace todo automáticamente?
- ¿Cómo se usa el DNI electrónico desde el ordenador? ¿Cómo se instala el lector de DNI?

Puesto que se trata de una firma electrónica, la firma debe realizarse obligatoriamente por medios electrónicos y se podrá realizar de dos formas:

- Descargando una aplicación en el PC: En este caso se utilizará para firmar la aplicación que habrá que instalar en el ordenador y no será necesario estar conectado a Internet. La aplicación a usar es AutoFirma, del Ministerio de Hacienda y Administraciones Públicas.
- 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. Pero también se pueden firmar los propios documentos en Internet utilizando el servicio ofrecido por VALIDe. Para firmar debe descargarse un componente que funciona sobre el mismo navegador.

En ambos casos es necesario disponer de un certificado electrónico.

Qué utilidad práctica tiene la firma electrónica

Aporta tres características en la comunicación por Internet: identificación del firmante, integridad de los datos y no repudio.

Pero aparte de eso, las aplicaciones prácticas de la misma son muchas y variadas, aunque, en general, están orientadas a realizar operaciones por Internet que en la vida cotidiana requieren de una firma para validarlas.

Algunos ejemplos de operaciones que se pueden realizar actualmente haciendo uso de la firma digital son:

- Realización de la Declaración de la Renta a través de Internet.
- Solicitudes en los registros electrónicos administrativos.
- Petición de la vida laboral.
- Recepción de notificaciones electrónicas.
- Firma de correos electrónicos.
- Firma de facturas electrónicas.

Centro de Tiflotecnología e Innovación - CTI
Camino de Hormigueras 172, Madrid 28031
T: (+34) 91 709 76 00 · F: (+34) 91 709 77 77
https://cti.once.es/

Accesibilidad a la hora de firmar un documento

El proceso de firma gráfica de un documento no es del todo accesible para una persona con ceguera usuaria de lector de pantalla, ya que el poder firmar o no un documento dependerá de cómo esté generado el mismo. Es decir, si cuenta con un lugar que esté correctamente identificado como aquel en el que se debe insertar la firma. De no ser así, los usuarios de lectores de pantalla no sabrán en qué parte del documento se debe insertar la firma.

Sin embargo, si se desea rubricar un documento mediante una firma no gráfica, la aplicación de Autofirma añadirá los datos de firma del usuario en el fichero, pero éstos no serán visibles en el documento. Este proceso, al no tener que seleccionar la ubicación de la firma en una localización concreta, sí es accesible.

Para verificar si un documento está firmado electrónicamente, pueden utilizarse las aplicaciones VALIDe o Adobe Acrobat, que, además, mostrarán los datos del registro de firma que contiene.

Centro de Tiflotecnología e Innovación - CTI
Camino de Hormigueras 172, Madrid 28031
T: (+34) 91 709 76 00 · F: (+34) 91 709 77 77
https://cti.once.es/

ENLACES DE INTERÉS

- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Orden HAP/800/2014, de 9 de mayo, por la que se establecen normas específicas sobre sistemas de identificación y autenticación por medios electrónicos con la Agencia Estatal de Administración Tributaria
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 6/2020, de 11 de noviembre, de servicios electrónicos de confianza
- REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
- Página de Inicio de la web de CERES
- Sección de Firma Electrónica del Portal Administración Electrónica
- Página web de la App Cl@ve
- Portal DNIe, web de la Dirección General de la Policía
- Autofirma, área de descargas
- VALIDe
- Firmar archivos PDF en Adobe Acrobat Reader
- Firmar archivos PDF online en Adobe.com
- Manual solicitud Certificado Persona Física CERES
- Guía Aplicación de Firma
- Firmar un documento PDF utilizando Adobe Acrobat Reader DC (web de CERES)
- Firmar un documento PDF utilizando Adobe Acrobat Reader DC (web de Adobe)