Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

Identidad Digital y Firma Electrónica: Facilitando la Relación con la Ciudadanía

¿Por qué es clave la identidad digital en las AAPP?

La identidad digital y la firma electrónica permiten identificar de forma fehaciente a los ciudadanos, empleados públicos o empresas que acceden a los servicios electrónicos

- La Ley 39/2015 reconoce el derecho de las personas a comunicarse electrónicamente con las Administraciones Públicas y establece como obligatoria la utilización de medios electrónicos entre administraciones y de las empresas con las administraciones. La identidad digital es el punto de entrada, y la firma electrónica la herramienta que permite completar trámites con plenas garantías jurídicas.
- La gestión de la identidad digital permite reforzar la seguridad, la trazabilidad y el cumplimiento normativo, al tiempo que mejora la experiencia del usuario

Pilares de la identidad electrónica

- **Autenticación:** Es el proceso mediante el cual un sistema verifica que el usuario es quien dice ser.

  Puede basarse en varios factores:
  - Algo que el usuario sabe (contraseña, PIN).
  - Algo que el usuario tiene (certificado digital, token, tarjeta criptográfica, OTP).
  - Algo que el usuario es (biometría: huella, reconocimiento facial, iris, etc.).

- **Autorización**: Controla el acceso a los recursos o servicios digitales una vez autenticada la identidad. Además, define qué puede hacer cada usuario dentro de un sistema.

Pilares de la identidad electrónica

- **Confianza:** La identidad debe estar soportada por un tercero de confianza (por ejemplo, un Prestador Cualificado de Servicios de Confianza - PSC según eIDAS).

  Implica validaciones previas (presenciales o remotas) y procedimientos normalizados.

- **Integridad:** Garantía de que los atributos de identidad no han sido alterados. Protección contra suplantación o manipulación de identidades.

- **Trazabilidad / Auditoría**: Registro seguro de los accesos y transacciones realizadas por la identidad. Permite verificar a posteriori el uso de los sistemas.

eIDAS

El **Reglamento eIDAS** (Reglamento UE 910/2014) es la normativa europea que regula la identificación electrónica, la autenticación y los servicios de confianza en las transacciones digitales dentro de la Unión Europea. Su objetivo es garantizar la interoperabilidad entre los sistemas de identificación y firma electrónica de los Estados miembros, permitiendo que ciudadanos, empresas y administraciones públicas puedan operar digitalmente en toda Europa con seguridad y validez legal.

eIDAS

Regula:

• **Identificación Electrónica**: Permite que los ciudadanos de cualquier país de la UE usen su sistema de identificación digital para acceder a servicios electrónicos (y en todos los países).

• **Firma Electrónica**: Regula los tipos de firma electrónica (simple, avanzada y cualificada) y le otorga validez legal equivalente a la firma manuscrita en toda la UE.

• **Sellos Electrónicos y Sellos de Tiempo**: Facilitan la certificación de documentos y transacciones digitales, la fecha y hora de la firma y posibilita la firma longeva

• **Prestadores de Servicios de Confianza**: Entidades certificadas que ofrecen servicios como emisión de certificados electrónicos, validación de firmas y cifrado de comunicaciones (FNMT, ACCV, Camerfirma, SIA, CatCer…)

eIDAS 2

eIDAS 2 es la **revisión del Reglamento eIDAS original (Reglamento (UE) 910/2014)** sobre identificación electrónica y servicios de confianza. Fue aprobado en 2024 y busca:

- **Crear una "Cartera Europea de Identidad Digital"** (European Digital Identity Wallet): cada ciudadano podrá tener una cartera digital europea en el móvil para identificarse y firmar digitalmente en toda la UE.
- **Reforzar la interoperabilidad** entre los sistemas de identificación electrónica de los Estados miembros.
- **Ampliar los servicios de confianza regulados** (por ejemplo, los registros electrónicos, servicios de prueba electrónica de atributos, etc.).
- **Mejorar la seguridad y control sobre los datos personales**: el usuario decide qué datos comparte.
- **Obligatoriedad para los Estados miembros**: deberán ofrecer la cartera de identidad digital a sus ciudadanos y empresas.

Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

Identidad Digital

Identidad digital

La identidad digital es el conjunto de atributos y credenciales electrónicas que permiten identificar a una persona física o jurídica en el ámbito digital. Es el equivalente funcional al DNI o a un poder notarial en el mundo físico. A través de ella, se pueden ejercer derechos, acceder a servicios y formalizar actos jurídicos.

Cuando hablamos de identidad digital tenemos que distinguir entre:

- Identificación: declaración de una identidad (por ejemplo, introducir el DNI).
- Autenticación: verificación de esa identidad (por ejemplo, mediante contraseña o certificado digital).
- Autorización: determinación de qué acciones puede realizar un usuario identificado.

Identidad digital. Medios reconocidos

Hay muchas formas de identificarse electrónicamente, con herramientas de terceros (Google y otras aplicaciones, credenciales bancarias, sistemas de OTP de tiendas y servicios on-line…..) pero solo 4 que aporten valor legal antes las AAPP

- El DNI electrónico, que incorpora un chip criptográfico que permite autenticar y firmar documentos y que contiene 2 certificados digitales
- Certificados digitales emitidos por los prestadores de servicios de certificación reconocidos
- La plataforma Cl@ve, con sus modalidades Cl@ve PIN (uso ocasional), Cl@ve Permanente (con segundo factor) y Cl@ve Firma (firma electrónica avanzada en la nube).
- Certificados de representación y registros electrónicos de apoderamientos, que permiten actuar en nombre de terceros (emitidos por prestadores de servicios de certificación reconocidos)

Identidad digital. Tipos de firma

La firma electrónica es un mecanismo legal y técnico que permite acreditar la identidad del firmante, garantizar la integridad del documento firmado y vincular jurídicamente al firmante con el contenido del acto. Tiene el mismo valor jurídico que una firma manuscrita cuando se cumplen ciertos requisitos.

La Ley 39/2015 reconoce todas ellas y establece su utilización según el tipo de procedimiento. Las Administraciones Públicas deben admitir cualquier firma electrónica reconocida conforme a la normativa europea, garantizando su interoperabilidad.

Identidad digital. Tipos de firma

1. Firma electrónica simple: cualquier método que permita vincular datos a una persona (ej. introducción de usuario y contraseña). Tiene validez limitada y se utiliza en contextos de bajo riesgo.

2. Firma electrónica avanzada: identifica al firmante de forma unívoca, permite detectar modificaciones posteriores en el documento y está vinculada solo a él. Se emplea en la mayoría de procedimientos administrativos.

3. Firma electrónica cualificada: es una firma avanzada realizada mediante un certificado cualificado y un dispositivo seguro de creación de firma. Tiene el mismo valor jurídico que la firma manuscrita (art. 25 del Reglamento eIDAS).

Identidad digital. Tipos de firma

Para facilitar su uso, existen herramientas como:

- @firma: plataforma de validación de certificados y firmas, gestionada por la Administración General del Estado.
- Cl@ve Firma: permite a los ciudadanos firmar electrónicamente desde cualquier dispositivo, sin necesidad de instalar certificados.
- Portafirmas electrónicos: sistemas corporativos que permiten a los empleados públicos firmar digitalmente con trazabilidad y control.
- Sistemas de copiado auténtico, sellado electrónico y archivo electrónico que garantizan la conservación legal de los documentos firmados.

Gestión de identidades

Además de la identidad digital ciudadana, las Administraciones deben gestionar las identidades internas: la de sus empleados, proveedores y colaboradores. Esto requiere un sistema robusto de gestión de identidades (IAM, por sus siglas en inglés) que controle el acceso a los sistemas de información, gestione roles y permisos y garantice la trazabilidad de las acciones.

Los sistemas de autenticación suelen basarse en directorios corporativos como LDAP o Active Directory, que permiten centralizar la administración de usuarios. Además, se integran con servicios como el correo electrónico, el gestor de expedientes o el portafirmas, garantizando una experiencia unificada mediante mecanismos como el SSO (Single Sign-On).

Gestión de identidades

Los principios básicos del control de acceso son:

- Autenticación: verificación de identidad del usuario.
- Autorización: definición de las acciones permitidas.
- Auditoría: registro de actividades para garantizar la trazabilidad.

Todo esto debe cumplir con el Esquema Nacional de Seguridad (ENS), especialmente en sistemas de categoría media y alta, y con la normativa de protección de datos (RGPD y LOPDGDD), que exige medidas técnicas y organizativas para evitar accesos indebidos y proteger la información personal.

Interreg
España – Portugal

Cofinanciado por la Unión Europea

IBERUS SMART

Ayuntamiento Ponferrada

Certificados digitales

¿Qué es un certificado digital?

Un **certificado digital** es un documento electrónico que asocia una identidad (persona física, jurídica o entidad) con una clave pública. Permite garantizar la identidad de los participantes en las transacciones electrónicas y asegurar la integridad y confidencialidad de la información intercambiada.

El certificado es emitido por una **Autoridad de Certificación (CA)**, que actúa como tercero de confianza, tras verificar la identidad del solicitante y que está en una TLS

- **Componentes básicos de un certificado digital:**
- **Identidad del titular:** nombre, NIF/NIE, razón social, etc.
- **Clave pública del titular:** vinculada a la identidad.
- **Datos de la CA:** nombre de la autoridad emisora.
- **Número de serie del certificado.**
- **Periodo de validez:** fecha de emisión y caducidad.
- **Algoritmo de firma y huella digital del certificado.**

¿Qué es un certificado digital?

Características principales

- **Identificación:** Permite autenticar de forma fiable la identidad del titular.
- **Confidencialidad:** Garantiza que la información solo pueda ser leída por el destinatario previsto (cuando se usa en cifrado).
- **Integridad:** Permite verificar que los datos no han sido alterados desde su emisión.
- **Autenticación:** Asegura que la persona que accede a un sistema o firma un documento es quien dice ser.
- **Validez jurídica:** En España, y según la normativa europea eIDAS, ciertos tipos de certificados permiten realizar firmas electrónicas con plena validez legal.
- **No repudio:** Impide que el firmante niegue posteriormente la autoría de la firma, siempre que se utilice de forma correcta y bajo condiciones de seguridad.

Características de un certificado digital

Identificación

Permite vincular de forma inequívoca una identidad (persona, empresa, administración pública, etc.) con un certificado digital emitido por una autoridad de certificación. El certificado contiene los datos de identidad verificados previamente.

Detalle técnico

- Nombre completo.
- NIF/CIF/NIE.
- Razón social (para empresas).
- Datos de la entidad emisora.

P.E.- Un funcionario del Ayuntamiento de Valladolid recibe un certificado digital de empleado público que le identifica como funcionario habilitado para realizar trámites electrónicos en nombre de la entidad.

Características de un certificado digital

Autenticación

Proceso mediante el cual el sistema verifica que quien presenta el certificado es realmente su titular legítimo.

Mecanismos habituales

- Contraseña personal de acceso al certificado.
- PIN asociado al dispositivo criptográfico.
- Biometría en sistemas más avanzados.

P.E.- El mismo funcionario accede a la plataforma de tramitación electrónica, accediendo con su certificado de empleado público, autenticándose como usuario autorizado, o utiliza su certificado para acceder a un tramite de la AGE vía Autentic@

Características de un certificado digital

Confidencialidad

Garantiza que la información cifrada solo pueda ser leída por el destinatario legítimo.

Mecanismos

- Cifrado de comunicaciones (SSL/TLS).
- Cifrado de mensajes o ficheros usando claves públicas y privadas.

P.E.- La documentación de un expediente sancionador es enviada cifrada al órgano instructor; solo los destinatarios autorizados pueden abrirla, aunque fuera interceptada.

Características de un certificado digital

Integridad

Permite asegurar que el contenido del documento o de los datos no ha sido alterado desde su firma.

Mecanismos

- Algoritmos hash (SHA-256, SHA-512...).
- Cálculo de huellas digitales de documentos.

P.E.- Cuando el funcionario firma electrónicamente una resolución, el sistema calcula un hash del documento. Si alguien lo modificara posteriormente, el hash no coincidiría y la alteración sería detectable.

Características de un certificado digital

No repudio

El firmante no puede negar posteriormente haber realizado la firma, siempre que la custodia de su clave privada haya sido segura.

Condiciones necesarias

- Control exclusivo de la clave privada por parte del firmante.
- Registro de auditoría y sellado de tiempo.

P.E.- Si el funcionario firma una adjudicación de contrato, no podrá alegar posteriormente que no la firmó, ya que sólo él tenía acceso a su clave privada protegida mediante su tarjeta criptográfica personal.

Características de un certificado digital

Validez jurídica

Otorga plena validez legal a los actos electrónicos, siempre que se utilicen firmas cualificadas o avanzadas bajo normativa eIDAS y nacional.

Normativas aplicables:

- Reglamento eIDAS (Reglamento UE 910/2014).
- Ley 6/2020 de servicios electrónicos de confianza.
- Ley 39/2015 para administraciones públicas.

P.E.- La firma electrónica cualificada de un contrato por parte de un proveedor y una administración pública tiene el mismo valor legal que una firma manuscrita.

Tipos de certificados digitales

Tipos de Certificados Digitales

Los certificados digitales pueden clasificarse en función de:

- **El titular (quién los usa)**
- **El uso o finalidad (para qué se usan)**
- **El nivel de seguridad (cómo se han emitido)**

Tipos de certificados digitales: por el titula

Persona física : Identifican a una persona en su propio nombre.
Usos: trámites personales, declaraciones fiscales, trámites administrativos, firma de contratos.
Ejemplo: certificado de ciudadano emitido por la FNMT.
Persona jurídica: Identifican a una empresa o entidad.
Usos: trámites fiscales, presentación de impuestos, registro mercantil, notificaciones electrónicas.
Ejemplo: certificado de representación de persona jurídica de la FNMT.
Representación legal / apoderados Permite a un representante actuar en nombre de otra persona o entidad.
Ejemplos: certificados de administrador único, certificados de apoderado general.
Empleado público (certificado de empleado o de pertenencia): Identifica al funcionario o empleado de una administración o entidad.
Usos: firma de resoluciones, expedientes, notificaciones oficiales.
Ejemplo: certificados emitidos por autoridades como FNMT, SIA, Camerfirma, ACCV..
E. Sello electrónico de entidad
Certifica a una entidad, pero sin personalización nominativa.
Usos: firma de documentos automatizados, sellado de registros, notificaciones masivas.

Tipos de certificados digitales: por su finalidad de uso

Certificados de autenticación: Permiten el acceso seguro a sistemas informáticos y aplicaciones.

Certificados de firma electrónica : Permiten firmar electrónicamente documentos con validez jurídica.

Certificados de cifrado (encriptación): Permiten cifrar correos electrónicos, ficheros o comunicaciones.

Certificados SSL/TLS : Para servidores web. Garantizan la seguridad de las conexiones en internet (https://).

Certificados de componente / servidor: Identifican sistemas o dispositivos concretos. Usos: integraciones entre sistemas, conexiones API seguras.

Tipos de certificados digitales: Por nivel de seguridad

Certificado cualificado
- Máximo nivel de seguridad.
- Emitido por Prestadores Cualificados de Servicios de Confianza.
- Requiere validación presencial o equivalente.
- Validez plena a efectos legales (firma cualificada = firma manuscrita).

Certificado avanzado
- Garantiza la identidad y control exclusivo de la clave privada.
- No requiere siempre validación presencial.
- Validez jurídica elevada, aunque no plena como la firma cualificada.

Certificado simple o básico
- Validaciones más laxas.
- Normalmente solo útil para autenticación de acceso a servicios.