

SISTEMAS Y MEDIOS DE IDENTIFICACIÓN DIGITAL I

En el contexto actual de transformación digital, la identificación electrónica es una piedra angular para garantizar la seguridad, legalidad y trazabilidad de las operaciones tanto con las Administraciones Públicas como con el sector privado.

El presente trabajo expone los medios legalmente reconocidos en España y la Unión Europea, su marco normativo y sus aplicaciones prácticas. El marco normativo de referencia está conformado tanto por legislación nacional, como europea:

A nivel de Legislación Nacional:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

Y como referentes de la Legislación Europea:

- Reglamento (UE) nº 910/2014 – Reglamento eIDAS (identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior).
- Directrices del ENISA sobre buenas prácticas en identificación electrónica.

La identificación electrónica ya no es una opción, sino un requisito legal y operativo. Conocer los medios existentes, su marco jurídico y sus implicaciones prácticas es esencial tanto para cumplir con la normativa como para aprovechar la digitalización de forma eficiente y segura.

La identificación electrónica se sustenta en distintos sistemas que garantizan la autenticación del usuario de manera segura y legal, permitiendo el acceso a servicios digitales y la firma de documentos con plena validez jurídica.

Todos los sistemas deben ajustarse a los niveles de seguridad definidos por el Reglamento eIDAS, que clasifica los medios de identificación en tres niveles: bajo, sustancial y alto.

Los sistemas de identificación legalmente reconocidos existentes en la actualidad son los siguientes:

1. Certificados Digitales (Basados en Infraestructura de Clave Pública – PKI). Los certificados digitales son credenciales electrónicas emitidas por una Autoridad de Certificación (CA) que vinculan una clave pública con la identidad de una persona física o jurídica. Existen los siguientes tipos:

- Certificado de Persona Física. Emitido habitualmente por la Fábrica Nacional de Moneda y Timbre (FNMT-RCM), aunque hay otros prestadores cualificados (Camerfirma, ANCERT...). Su funcionamiento es relativamente sencillo.
 - El usuario solicita el certificado online y verifica su identidad presencialmente (en oficinas de la AEAT o entidades acreditadas).
 - Se instala en el navegador o en una tarjeta criptográfica.
 - Se utiliza para firmar digitalmente y autenticarse en portales públicos y privados, así como la presentación de impuestos, consulta de vida laboral, solicitud de becas, recursos administrativos y un sinnúmero de actos y procedimientos con las administraciones públicas.
- Certificado de Representante Legal. Se vincula a la empresa mediante los poderes inscritos en el Registro Mercantil. La FNMT o Camerfirma verifican la representación mediante el certificado registral. El funcionamiento es muy similar al certificado de persona física. Presenta tres modalidades principales:
 - Representante para Administrador Único/Solidario.
 - Representante para Persona Jurídica.
 - Representante para Entidad sin Personalidad Jurídica.
- Certificado de Empleado Público. Asigna la identidad profesional a un empleado en su relación con la Administración. Uso exclusivo: firma de resoluciones, notificaciones, trámites internos. Generalmente es emitido por la propia administración o mediante convenios con la Fábrica Nacional de Moneda y Timbre.

2. DNI Electrónico (DNLe). El DNLe es un documento nacional de identidad que incorpora un chip criptográfico con certificados electrónicos. Autentica al titular y permite firmar con validez jurídica. Incluye Certificado de autenticación y Certificado de firma electrónica. A nivel de funcionamiento, requiere lector de tarjetas criptográficas y software compatible (AutoFirma, DNLeRemote) e introducción del PIN por el usuario. Su uso ha disminuido frente a Cl@ve por la necesidad de hardware adicional.

3. Sistema Cl@ve. Sistema de autenticación centralizado impulsado por la AGE para unificar el acceso a los servicios públicos. Presenta tres versiones posibles, en función del nivel de seguridad requerido: bajo, medio y alto.

- Cl@ve PIN. Nivel de seguridad: bajo. Sistema de contraseña de un solo uso (OTP), con validez limitada en el tiempo. No requiere instalación, ni ningún tipo de certificado. Su funcionamiento es el siguiente:
 - Solicitud de un PIN temporal mediante la app Cl@ve o SMS.
 - Se combina con el NIF y una contraseña de registro previo.
 - Ideal para usuarios ocasionales.
- Cl@ve Permanente. Nivel de seguridad: sustancial. Basado en usuario + contraseña y verificación en dos pasos (doble factor). Funcionamiento:
 - Registro presencial o con certificado digital.
 - Uso habitual por empleados públicos o ciudadanos que acceden de forma continua.
 - Se puede complementar con autenticación mediante app o SMS.
- Cl@ve Firma. Nivel de seguridad: alto. Permite la firma electrónica avanzada centralizada (sin instalar certificados en local).Funcionamiento:
 - Se vincula a una cuenta Cl@ve Permanente.
 - El certificado se encuentra alojado de forma segura en un servidor remoto de la Administración (HSM).
 - El usuario firma mediante validación por app o código de seguridad.
 - Firma documentos con plena validez legal sin necesidad de dispositivos físicos.