TEMA 080

IDENTIFICACIÓN Y FIRMA ELECTRÓNICA (1) MARCO EUROPEO Y NACIONAL. CERTIFICADOS DIGITALES. CLAVES PRIVADAS, PÚBLICAS Y CONCERTADAS. FORMATOS DE FIRMA ELECTRÓNICA. PROTOCOLOS DE DIRECTORIO BASADOS EN LDAP Y X.500. OTROS SERVICIOS.

Versión	30.1
Fecha de actualización	12/10/2024

ÍNDICE

1. Firma Electrónica

1.1 Firma Electrónica y Firma Digital

- **Firma electrónica:** Según el Artículo 3 del Reglamento Europeo de Identificación electrónica y servicios de confianza 910/2014 (eIDAS), son "los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar".

  Este es por tanto un **concepto jurídico** que se sirve de diversos soportes electrónicos, como un lápiz electrónico o una **firma digital**, y da fe de la voluntad del firmante.

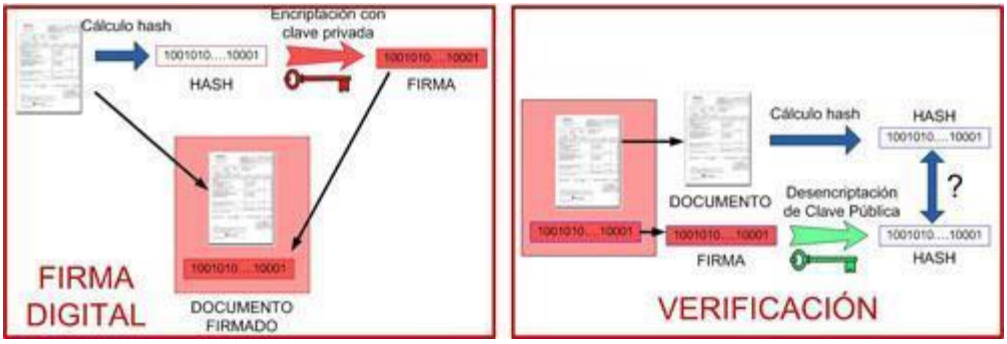
- **Firma digital**: Es el valor o conjunto de caracteres, calculado criptográficamente a partir de unos datos, que permiten **verificar la integridad, autenticidad y no repudio** de dichos datos, denominados como "mensaje".

  En este caso, es un **concepto tecnológico**, que se basa en sistemas de criptografía de clave pública (*PKI - Public Key Infrastructure*).

La firma digital sirve para identificar al emisor de dicho mensaje (autenticidad) y certificar que el documento no se ha modificado (integridad) con respecto al original. No se puede negar haberlo firmado (no repudio en origen), puesto que esta firma utilizará un certificado emitido por una autoridad de certificación (CA), y podrá ser validada por una autoridad de validación. Por lo tanto, establece una vinculación unívoca entre el firmante, los datos firmados y la firma. La firma digital no garantiza la confidencialidad.

1.1.1 Proceso de firma y validación

La firma digital utiliza cifrado asimétrico que es la base de la PKI. Los pasos a seguir para realizar una firma y verificarla en el receptor son los siguientes:



Proceso de firma:

- Se calcula el hash del mensaje a firmar.
- Se encripta el hash del mensaje con la clave privada del emisor (ésta es la firma)
- Se envían al receptor el documento original junto con la firma.

Proceso de validación:

- En el receptor, se calcula de nuevo el hash del mensaje original.
- Se utiliza la clave pública del emisor para desencriptar la firma.
- Se compara el hash calculado con el desencriptado, si coinciden se ha mantenido la integridad y se garantiza el no repudio.

Si en la firma se ha recibido la parte pública del certificado electrónico, debe validarse para comprobar que se trata de un certificado cualificado y que no está revocado. De esta forma se garantiza la autenticidad y el no repudio.

Modos de firma por múltiples firmantes:

- Cofirma: firma en paralelo (dos firmantes de un mismo documento, al mismo nivel).
- Contrafirma (refrendo de firma): firma en cascada (la última firma refrenda la anterior).

Problema de la criptografía de clave pública → incertidumbre de que la clave pública pertenezca realmente a la persona que dice poseerla.
Solución → Dar certidumbre a la identidad, un tercero de confianza que garantice la relación entre la clave utilizada y la identidad real de su dueño (certificados digitales) mediante redes de confianza centralizadas o descentralizadas (PKIs).

1.1.2 Claves Públicas, privadas y concertadas

Todo usuario que quiera realizar una firma electrónica dispondrá de dos claves, una **clave privada** (que nunca sale de su PC tras ser generada y se utilizará para firmar), y una **clave pública** (que se comparte con el receptor y es utilizada para poder verificar quién fue el firmante). Esto se denomina criptografía asimétrica o de clave pública y se basa en la existencia de un tercero de confianza (explicado en detalle en el Tema 81).

Las claves concertadas son datos proporcionados por la Administración que sólo el interesado debe conocer, por ejemplo, usuario/contraseña, casilla N de la declaración de la Renta, fecha de expedición del DNI, etc. Los sistemas de **clave concertada** se aceptan como sistema de identificación en el **Art.9.2.c) de la Ley 39/2015**, siempre que cuenten con el registro previo del usuario, registro durante el cual se acuerda una clave a usar con el proveedor y que garantiza la identidad del usuario, sin ser necesario un certificado electrónico. Un ejemplo sería Cl@ve Permanente o cualquier otro sistema de usuario-contraseña.

1.2 Certificado Digital

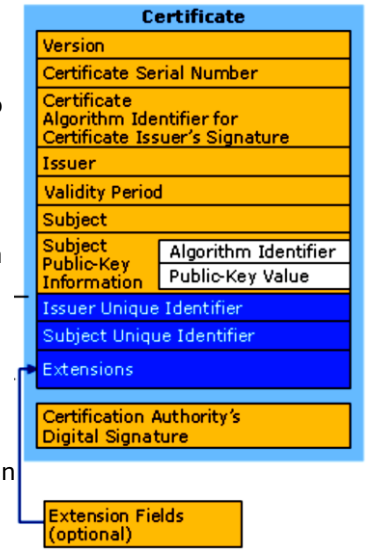
El **certificado digital** es un documento electrónico, expedido y firmado por una tercera parte de confianza, que vincula una clave pública con la identidad del propietario de la clave privada complementaria.

1.2.1 Estructura de los Certificados

El **estándar X.509 v3** es el estándar de la ITU-T para infraestructuras de clave pública, y especifica la estructura y formato de los certificados digitales de clave pública, de las listas de revocación de certificados (CRL) y de los certificados de atributos. Esta estructura y formato ha sido adoptado por el IETF (RFC 5280) y es conocido como **PKIX**.

Los certificados X.509 v3 emplean el lenguaje ASN.1 (*Abstract Syntax Notation One*) y su estructura tiene los siguientes campos:

- Version
- Serial number: identificador del certificado, único para cada CA.
- Signature algorithm: algoritmo empleado por la CA para firmar el certificado
- Issuer: nombre de la tercera parte de confianza (CA) que lo expide
- Validity period: periodo de validez de las claves (desde – hasta)
- Subject: sujeto titular vinculado a la clave pública (en notación DN)
- Subject Public Key Information: clave pública y algoritmo usado para crearla (lo que la ley incluye en los "**datos de verificación de firma**")
- Extensions: permiten una gran flexibilidad. Constan de tres partes: "*Extensión ID*", "*Critical*" y "*Value*"
  - *Subject Alternative Name* → identidades adicionales, seudónimos
  - *Authority Information Access* → enlaces al servidor **OCSP** de la VA
  - *CRL distribution points* (CDP) y *Freshest CRL* (*Delta CRL* dist. point) → en CRL



  - *Key Usage* → Uso del certificado, fuente de problemas de interoperabilidad
    - *digitalSignature* → para autenticación
    - nonRepudiation / ContentCommitment → para firma digital
    - keyCertSign → para certificados de CA
- Issuer digital signature: firma de la tercera parte de confianza (autofirmado)

1.2.2 Validación de Firma Digital con Certificado

Para validar una firma digital no basta con validar la firma en sí, también es necesario validar el certificado asociado. Para ello, la Autoridad de Certificación (CA) emisora de un certificado electrónico está obligada a ofrecer una Autoridad de Validación (VA). En concreto, se requiere validar:

- Los límites de uso del certificado
- El periodo de validez
- El estado de vigencia del certificado, ya que éste puede haber sido revocado o suspendido de forma temporal, antes de vencer el periodo de validez.

1.2.3 Validación de Certificados

Existen diferentes técnicas para validar el estado y la vigencia de un certificado electrónico:

- **CRL** (*Certificate Revocation List*):
  - Las CAs mantienen, firman y publican **listas** con los números de serie de los **certificados que han sido revocados** (antes de su expiración) y su **fecha de revocación**. Estas listas (CRLs) se publican en repositorios HTTP o LDAP cuya ubicación es indicada en la extensión *CDP (CRL Distribution Point)* del certificado a validar.
  - Existen varios métodos para la consulta de CRLs:
    - **Muestreo periódico de CRL**
    - **Anuncio de CRLs** por la CA cada vez que se modifica la CRL
    - **Verificación en línea**, obteniendo la CRL cada vez que se requiere una validación
  - Para mitigar el problema que supone el crecimiento de la CRL, se emplean "***delta-CRL***" (*Freshest CRL*) → certificados revocados desde la publicación de la última CRL de base.

- **OCSP** (*Online Certificate Status Protocol*, RFC 6960):
  - El protocolo permite consultar a la Autoridad de Validación (VA) el estado de un certificado
  - Los mensajes del protocolo se codifican en ASN.1 y se envían sobre HTTP
    - Las peticiones contienen el número de serie del certificado a validar, así como el hash de nombre de la CA que lo emitió y su clave pública
    - La respuesta, que va firmada y con sello de tiempo, puede ser *good, unknown* o *revocked*.
    - El uso de *nonces* en peticiones y respuestas permite evitar ataques de *replay*
  - ***Desventaja***: para altos volúmenes de tráfico, muchas respuestas OCSP
  - ***Solución***: **OCSP Stapling** → el servidor web (NO el cliente) consulta regularmente a la VA, acumula respuestas firmadas y selladas sobre validez y las "grapa" en la respuesta al cliente.

1.3 Formatos de Firma electrónica

Independientemente del algoritmo de firma empleado (hash y cifrado asimétrico), existen diferentes formatos estandarizados para la firma electrónica:

- ***PKCS#7 / CMS (****Cryptographic Message Syntax, RFC 2315 / RFC 5652****)***

Permite diferentes tipos de objetos: data, signed-data, enveloped-data, signed-and-enveloped-data, digested-data y encrypted-data.

- ***CAdES (****CMS Advanced Electronic Signature****) – ETSI TS 103173 v.2.2.1***

Definido para firma de cualquier tipo de documento. Permite tanto *attached signature*, como *detached signature*.

- **XMLDsig**
  - Define una sintaxis XML para soporte a la firma digital.
  - Permite firmar cualquier tipo de recurso, no solo XML.
  - Existen varios modos: *detached signature*, *enveloped signature* y *enveloping signature*.
- ***XadES (****XML Advanced Electronic Signature****) – ETSI TS 103171 v.2.2.1***
  - Firma de documentos XML.
  - Permite *enveloping*, *enveloped* y *detached* signature.
- ***PadES (****PDF Advanced Electronic Signature****) – ETSI TS 103172 v.2.2.2***
  - Para firma de documentos PDF.
  - *Permite un formato Avanzado de firma*: PadES LTV (Long Term Validation): firma longeva con resellado
- ***S/MIME*** *(Secure / Multipurpose Internet Mail Extensions)*: ***Proporciona firma electrónica en correos electrónicos***
- **AsiC** (Associated Signature Container)
  - Define una estructura de contenedor para englobar: archivo, firma y sello de tiempo
  - El contenedor está basado en zip

La **firma longeva** es aquella que incluye las evidencias de validación en la propia estructura de firma, es decir: Firma longeva = firma simple + resultado de la validación del certificado.

De este modo se definen formatos avanzados de firma, para garantizar el instante de tiempo en el que se realiza la firma y su longevidad. Son incrementales.

CAdES y XadES:

- T (Timestamp): Con sello de tiempo.
- C (Completo): con referencias a datos de verificación (certificados y listas de revocación).
- X (Extendido): añade sellos de tiempo a las referencias incluidas en el tipo C.
- XL (Extendido longevo): Añade certificados y listas de revocación al documento firmado para permitir su validación en el futuro.
- A (Archivo): Añade la posibilidad de resellado periódico.

PadES:

- LTV (Long Term Validation): Firma longeva en un documento PDF permitiendo su resellado.

Adicionalmente han surgido los formatos baseline con el objetivo de unificar los formatos avanzados.

Formato Baseline	Definición	CAdES	XAdES	PAdES
B	Firma sin formato avanzado	BES y EPES		
T	Firma con sello de tiempo	T		
LT	Firma T con certificados	XL		

	cadena confianza y evidencias		
LTA	Firma LT con sellado de evidencias. Validez a largo plazo de la firma.	A	LTV

Cuando finaliza la vigencia de un certificado, no se puede verificar si ese certificado era válido en el momento de la firma si no se ha guardado evidencia de ello. Las firmas longevas incluyen un sello de tiempo para asegurar el momento en el que se hizo la validación, de forma que su longevidad está determinada por la longevidad del sello de tiempo, y por tanto se requerirá re-sellado antes de que caduque el certificado que se usó para el sello de tiempo (TS@).

1.4 Definiciones Firma Electrónica y Certificados de Firma

Definiciones relativas a la firma electrónica: (definiciones del Reglamento eIDAS 910/2014)

- ***Firmante**: **persona física** que crea una firma electrónica.*
- ***Firma electrónica**: datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.*
- ***Firma electrónica avanzada**: firma electrónica que cumple los requisitos siguientes:*
  - *Estar vinculada al firmante de manera única.*
  - *Permitir la identificación del firmante.*
  - *Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y*
  - *Estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable*
- ***Firma electrónica cualificada**: firma electrónica avanzada que se crea mediante un **dispositivo cualificado** de creación de creación de firmas electrónicas y que se basa en un **certificado cualificado** de firma electrónica.*

Definiciones relativas a los dispositivos de creación de firma:

- ***Dispositivo de creación de firma:** equipo o programa informático configurado que se utiliza para crear una firma electrónica.*
- ***Dispositivo cualificado de creación de firma electrónica**: dispositivo de creación de firmas electrónicas que cumple los requisitos* siguientes:
  - *esté garantizada razonablemente la **confidencialidad de los datos de creación** de firma electrónica utilizados para la creación de firmas electrónicas,*
  - *los datos de creación de firma electrónica utilizados para la creación de firma electrónica **sólo puedan aparecer una vez en la práctica,***
  - *exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica **no pueden ser hallados por deducción** y de que la firma está **protegida** con seguridad **contra la falsificación** mediante la tecnología disponible en el momento,*
  - *los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser **protegidos por el firmante legítimo de forma fiable frente a su utilización por otros**.*
  - *Otros requisitos (indicados en el anexo II del Reglamento eIDAS)*

El Reglamento **2024/1183 (eIDAS 2)** incluye la siguiente definición:

- ***Dispositivo cualificado de creación de firma electrónica a distancia:** dispositivo cualificado de creación de firmas electrónicas que está gestionado por un prestador cualificado de servicios de confianza, de conformidad con el artículo 29 bis, en nombre de un firmante;*

Definiciones relativas a los certificados de firma electrónica:

- ***Certificado de firma electrónica**: declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o seudónimo de esa persona*
- ***Certificado cualificado de firma electrónica**: certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos* siguientes:
  - Indicar, al menos en formato MP (procesable automáticamente), si ha sido expedido como certificado cualificado
  - Indicar, al menos en formato MP, si los datos de validación se encuentran en un dispositivo cualificado de firma.
  - *Contener* el nombre del firmante o, en su caso, un seudónimo claramente establecido como tal.
  - Otros *requisitos (anexo I del Reglamento eIDAS)*

Efecto jurídico de la firma electrónica y reconocimiento:

- *Una firma electrónica cualificada tendrá un **efecto jurídico equivalente al de una firma manuscrita**.*
- *Una firma electrónica cualificada basada en un certificado cualificado emitido en un estado miembro será reconocida como una firma electrónica cualificada en **todos los demás Estados miembros**.*

1.5 Lista de Servicios de confianza (TSL)

Se trata de una lista de confianza de **prestadores de servicios de certificación** que expiden certificados cualificados de acuerdo a la normativa vigente.

- Deben cumplir las especificaciones técnicas de la Decisión 2013/662/UE y la especificación técnica ETSI TS 119 612: *Electronic Signatures and Infrastructures (ESI); **Trusted Lists***
- **Firmadas con certificados electrónicos específicos para este uso**, comunicados a la Comisión Europea para que se pueda comprobar su autenticidad e integridad.

La **CE mantiene una relación de listas TSL de los EEMM** → List of Trusted Lists (LoTL). También en formatos HR y MP: https://digital-strategy.ec.europa.eu/en/policies/eu-trusted-lists

LEGISLACIÓN RELACIONADA:

- **Directiva 2006/123/CE** relativa a los servicios en el mercado interior → se debe facilitar el uso transfronterizo de las ventanillas únicas.
- **Reglamento (UE) 910/2014 (eIDAS)** → establece que **en la TSL tienen que estar los servicios de confianza cualificados** prestados por los Prestadores Cualificados de Servicios de Confianza – PCSC
  - → **Cada EEMM de la UE establecerá, mantendrá y publicará su Lista de Confianza** de sus PSC supervisados/ acreditados que emiten certificados reconocidos.
- **La Ley 6/2020 de servicios electrónicos de confianza**, establece en su artículo 9 apartado 3 que los prestadores de servicios de confianza deberán comunicar al Ministerio de Asuntos Económicos y Transformación Digital en los términos previstos en el artículo 20.1 del Reglamento (UE) 910/2014, el inicio de su actividad, así como información relativa a los servicios que prestan y sus correspondientes certificaciones de calidad.

TSL EN ESPAÑA:

El Ministerio de Transformación Digital y Función Pública elabora dicha TSL (en HR y MP) que contienen los PSC supervisados / acreditados en España: Sede electrónica del Ministerio para la Transformación Digital y de la Función Pública - Lista de confianza de prestadores cualificados de servicios electrónicos de confianza (mineco.gob.es)

2. Sello electrónico

El sello electrónico es el modelo de firma electrónica para las personas jurídicas. Para ello, se utiliza un certificado electrónico de sello.

Definiciones relativas al sello electrónico*: (definiciones Reglamento eIDAS)*

- ***Creador de un sello**: **persona jurídica** que crea un sello electrónico*
- ***Sello electrónico*** (definiciones semejantes a la firma electrónica)
- ***Sello electrónico avanzado***
- ***Sello electrónico cualificado*** (*un sello electrónico cualificado debe ser creado por un dispositivo electrónico cualificado y basarse en un certificado cualificado de sello electrónico).*

Definiciones relativas a los certificados de sello electrónico:

- ***Certificado de sello electrónico***
- ***Certificado cualificado de sello electrónico.***
  - *al menos, el nombre del creador y, cuando proceda, su número de registro oficial.*

El Reglamento **2024/1183 (eIDAS 2)** incluye la siguiente definición:

- ***Dispositivo cualificado de creación de sello electrónico a distancia:** dispositivo cualificado de creación de sellos electrónicos que está gestionado por un prestador cualificado de servicios de confianza, de conformidad con el artículo 39 bis, en nombre de un creador de sellos;*

Desde el 1 de julio de 2016 (inicio cumplimiento eIDAS) no se emiten certificados de persona jurídica. Han sido sustituidos por:

- **Certificado de persona física representante de persona jurídica.**
- **Certificado de persona física representante de entidad sin personalidad jurídica.**

3. Sello de tiempo electrónico

- ***Marca de tiempo*: la mera** referencia temporal asociada a un documento (distinta a sello de tiempo, donde interviene un prestador de servicios de confianza que asegura la exactitud del momento temporal).

- ***Sello de tiempo electrónico*:** datos en formato electrónico que **vinculan otros datos** en formato electrónico **con un instante concreto**, aportando la prueba de que estos últimos datos existían en ese instante.

Si no se tuviese este sello de tiempo habría que realizar la consulta del estado de revocación del certificado con respecto al momento de la validación. De ese modo, podría darse el caso de que la firma hubiese sido válida, pero sin embargo la validación de resultado negativo por haber sido el certificado revocado durante el periodo transcurrido entre la firma y la validación de ésta.

- ***Sello cualificado de tiempo electrónico (art. 42.1 Reglamento 910/2014)***:
  - Vincular la fecha y hora con los datos de forma que se **elimine la posibilidad de modificar** los datos sin que se detecte.
  - Basarse en una fuente de información temporal vinculada al **Tiempo Universal Coordinado.**
  - Haber sido firmada mediante el uso de **firma electrónica avanzada o sellada** con un sello electrónico avanzado del **prestador cualificado de servicios de confianza** o por cualquier método equivalente.

El **Reglamento 2024/1183** incluye el siguiente apartado.

- *1 bis. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la vinculación de la fecha y hora con los datos y exactitud de la fuente de información temporal sea conforme a las*

normas, las especificaciones y procedimientos a que se refiere el apartado 2.»;

- *A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para la vinculación de la fecha y hora con los datos y para el establecimiento de la exactitud de las fuentes de información temporal. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.*

Las Administraciones Públicas disponen de la **TSA** como Autoridad de Sellado de Tiempo, sincronizada con el Real Observatorio de la Armada (ROA) y ofrecido por el servicio @firma a través de la Red Sara.

4. Certificados de Autenticación de sitio web

- ***Certificado de autenticación de sitio web**: declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado*
- ***Certificado cualificado de autenticación de sitio web***
  - *se expide a una persona física o jurídica, identificada en el propio certificado*
  - *deberá aparecer al menos su ciudad y estado*
  - *Naturalmente, el certificado contendrá el/los nombre/s de dominio explotados por la persona física o jurídica a la que se expida el certificado.*

5. Marco Regulatorio

5.1 Marco Europeo

5.1.1 Reglamento UE 910/2014 (EIDAS)

Reglamento 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 por el que se deroga la Directiva 1999/93/CE

Relación de artículos más destacados:

- Artículos sobre firma electrónica y certificados de firma electrónica: 3 (9-15), 25, 26 y Anexo I
- Artículos sobre sello electrónico y certificados de sello electrónico: 3 (24-30), 35, 36 y Anexo III
- Artículos sobre dispositivos de creación de firma: 3 (22 y 23) y Anexo II
- Artículos sobre sellos de tiempo: 3 (33 y 34), 41 y 42
- Artículos sobre certificados de autenticación de sitio web: 3 (38 y 39) y anexo IV
- Artículos sobre entrega certificada: 3 (36 y 37) y sección 7 (arts 43 y 44).

Si un Estado miembro **requiere una firma electrónica avanzada** con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá

- las firmas electrónicas avanzadas,
- las firmas electrónicas avanzadas basadas en un certificado cualificado de firma electrónica y
- las firmas electrónicas cualificadas

por lo menos en los formatos o con los métodos definidos en los 4 actos de ejecución indicados abajo.

Si un Estado miembro **requiere una firma electrónica avanzada basada en un certificado cualificado** con el mismo fin, dicho Estado miembro reconocerá

- las firmas electrónicas avanzadas basadas en un certificado cualificado de firma electrónica y
- las firmas electrónicas cualificadas

por lo menos en los formatos o con los métodos definidos en los 4 actos de ejecución indicados abajo.
La aplicación del Reglamento eIdAS, implica la puesta en marcha de 8 actos ejecutivos a adoptarse en un año:

4 **actos de ejecución** relativos a la identificación y autenticación digital (eID):

- *Cooperación entre los EEMM (art. 12.7)* → *Decisión de Ejecución (UE) 2015/296*
- *Marco de Interoperabilidad (art. 12.8)* → *Reglamento de Ejecución (UE) 2015/1501*
- *Niveles de garantía (seguridad) de eID (art. 8.3)* → *Reglamento de Ejecución (UE) 2015/1502*
- *Identificación en las notificaciones (art. 9.5)* →*Decisión de Ejecución (UE) 2015/1984*

4 **actos de ejecución** en materia de servicios de confianza digital:

- *Formatos de firma electrónica (art. 27.4)* → *Decisión de Ejecución (UE) 2015/1506*
- *Formatos de sellos electrónicos (art. 37.4)*
- *Listas de confianza (art. 22.5)* → *Decisión de Ejecución (UE) 2015/1505*
- *Marca de confianza de la UE (art. 23.3)* →*Reglamento de Ejecución (UE) 2015/806*

Los Estados miembros **no exigirán** para la utilización transfronteriza de un servicio en línea ofrecido por un organismo del sector público una firma electrónica cuyo nivel de garantía de la seguridad sea **superior al de una firma electrónica cualificada**.

5.1.2 Decisión de Ejecución (EU) 2015/1506: Formatos Reconocidos

Decisión de ejecución (EU) 2015/1506 *de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los* ***formatos de las firmas electrónicas avanzadas y los sellos avanzados*** *que* ***deben reconocer*** *los* ***organismos del sector público****.*

Establece que los Estados Miembros reconocerán los formatos **XAdES, CAdES o PAdES** en niveles de conformidad B, T o LT (XL), y los contenedores **ASiC.**

5.1.3 Reglamento UE 2024/1183 (EIDAS 2.0)

Reglamento UE 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024 por el que se modifica el Reglamento (UE) n.o 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.

Publicado en el DOUE el 30 de abril de 2024 con entrada en vigor el 20 de mayo de 2024.

5.1.3.1 Principales modificaciones respecto al reglamento UE 910/2014.

- El punto 16 del Art. 3 se modifica como sigue:

16) ***"servicio de confianza",*** *servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en cualquiera de las actividades siguientes:*

  - *la expedición de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza;*
  - *la validación de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza;*
  - *la creación de firmas electrónicas o sellos electrónicos;*
  - *la validación de firmas electrónicas o sellos electrónicos;*

- *la conservación de firmas electrónicas, sellos electrónicos, certificados de firma electrónica o certificados de sello electrónico;*
- *la gestión de dispositivos de creación de firma electrónica a distancia o dispositivos de creación de sello electrónico a distancia;*
- *la expedición de declaraciones electrónicas de atributos;*
- *la validación de declaraciones electrónicas de atributos;*
- *la creación de sellos de tiempo electrónicos;*
- *la validación de sellos de tiempo electrónicos;*
- *la prestación de servicios de entrega electrónica certificada;*
- *la validación de los datos transmitidos a través de servicios de entrega electrónica certificada y las pruebas correspondientes;*
- *el archivo electrónico de datos y documentos electrónicos;*

- Se incorporan como servicios de confianza la **expedición y validación de declaraciones electrónicas de atributos, la gestión de dispositivos de creación de firma o sello electrónico a distancia y el archivo electrónico.**
- En el art. 3, entre otras definiciones, se incluyen los puntos relativos a la cartera europea de identidad digital, atributos, declaración electrónica de atributos, fuente auténtica y libro mayor electrónico.

*42) **"cartera europea de identidad digital",** medio de identificación electrónica que permite al usuario almacenar, gestionar y validar de forma segura datos de identificación de la persona y declaraciones electrónicas de atributos con el fin de proporcionarlos a las partes usuarias y a otros usuarios de carteras europeas de identidad digital, así como firmar por medio de firmas electrónicas cualificadas o sellar por medio de sellos electrónicos cualificados;*

- En el **Capítulo II**, se inserta la **Sección 1 para la descripción detallada de la Cartera Europea de Identidad Digital,** partes usuarias de las mismas, proceso de certificación, publicación de lista de carteras europeas de identidad digital certificadas y compromiso de la seguridad de las carteras europeas de identidad digital.
- Se incluye el cumplimiento del artículo 21 de la Directiva (UE) 2022/2555 tanto a los prestadores de servicio de confianza (art. 19) no cualificados como cualificados (art. 20).
- Se incluye el art. 29 bis. **Requisitos aplicables a un servicio cualificado para la gestión de dispositivos cualificados de creación de firma electrónica a distancia.**
- En el **Capítulo III**, se insertan las siguientes secciones:
  - **Sección 9 para la Declaración electrónica de atributos**
  - **Sección 10 para los Servicios de Archivo electrónico**
- Se inserta el **Capítulo IV bis**, donde se describe el **Marco de Gobernanza** tanto para la supervisión del marco de la cartera europea de identidad digital como para los servicios de confianza. Se define el Grupo de Cooperación sobre la Identidad Digital Europea.
- Se incluyen los Anexos siguientes:
  - Anexo V: Requisitos aplicables a la declaración electrónica cualificada de atributos
  - Anexo VI: Lista mínima de atributos.
  - Anexo VII: Requisitos aplicables a la declaración electrónica de atributos expedida por un organismo público responsable de una fuente auténtica o en nombre de este.
- A más **tardar el 21 de noviembre de 2024**, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos aplicables a los

requisitos a que se refieren diferentes apartados del presente artículo sobre:

- La implantación de las carteras europeas de identidad digital.
- Normas de referencia, especificaciones y procedimientos para la certificación de las carteras europeas de identidad digital.
- Compromiso de la seguridad de las carteras europeas de identidad digital.
- Verificación transfronteriza de identidades.
- Requisitos para la declaración electrónica cualificada de atributos y frente a fuentes auténticas.

5.1.3.2 Resumen

- Para 2026, cada Estado miembro deberá poner a disposición de sus ciudadanos una cartera de identidad digital (EDIW) y aceptar EDIW de otros Estados miembros de acuerdo con la normativa revisada.
- Se han incluido suficientes salvaguardas para evitar la discriminación de aquellas personas que decidan no utilizar la cartera digital, que seguirá siendo siempre voluntaria.
- El modelo de negocio de la cartera digital: emisión, uso y revocación será gratuito para todas las personas físicas.
- En lo que se refiere a la validación de la atestación electrónica de atributos, los EEMM deberán proporcionar mecanismos de validación gratuitos únicamente para verificar la autenticidad y validez de la cartera digital y de la identidad de las partes confiables.
- Los componentes del software de aplicación de las carteras digitales serán de código abierto, pero se concede a los EEMM un margen de maniobra para que, por razones justificadas, no sea necesario revelar componentes específicos distintos de los instalados en los dispositivos de los usuarios.

5.2 Marco regulatorio en España

Relación de normas y artículos más destacados:

- **Ley 39/2015, del procedimiento administrativo común de las AAPP:** Título I – Capítulo II
- **Ley 40/2015, del Régimen Jurídico del Sector Público:** artículos 42, 43, 45
- **ENS:** Art. 33 y medida mp.info.4 → relativas al uso de firma electrónica.
- **ENI** y **NTI** de Política de firma electrónica y de certificados de la Administración.
- **Resolución de 14 de julio de 2017**, de la Secretaría General de Administración Digital por la que se establecen las condiciones de **uso de firma electrónica no criptográfica** en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.
- **Ley 6/2020**, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- **Orden ETD/465/2021**, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, modificada por la orden **ETD/743/2022**.

5.2.1 Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de Confianza

Regula aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (artículo 1: objeto de la Ley).

Aplica a prestadores de servicios de confianza públicos y privados establecidos en España y a los prestadores de otro Estado que tengan un establecimiento permanente en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea (artículo 2: ámbito de aplicación).

Introduce la posibilidad de comprobar la identidad a distancia mediante métodos como la videoconferencia o la vídeo-identificación (artículo 7.2):

> *Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad. La determinación de dichas condiciones y requisitos técnicos se realizará a partir de los estándares que, en su caso, hayan sido determinados a nivel comunitario.*

- *Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, modificada por la orden ETD/465/2022.*

Relación de artículos más destacados:

- Título II: Certificados electrónicos (artículos 4-7).
- Título III: Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza (artículos 8-13).
  - Los prestadores de servicios de confianza no cualificados pueden iniciar su actividad sin necesidad de verificación administrativa previa de cumplimiento de requisitos, pero deben comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses desde que la inicien.
- Título IV: Supervisión y control (artículo 14).
  - Órgano de supervisión: Ministerio de Asuntos Económicos y Transformación Digital
- Título V: Infracciones y sanciones (artículos 18-20).

5.2.2 Ley 39/2015: Firma de los interesados

Artículo 10. Sistemas de firma admitidos por las AAPP

[...] 2. En el caso de que los interesados optaran por relacionarse con las AAPP a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica
- **cualificada** y **avanzada**
- **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 de sello electrónico
- **cualificado** y **avanzado**
- **basados en certificados** electrónicos **cualificados** de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Cualquier **otro sistema** que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital.

[...] 4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las AAPP **podrán admitir los sistemas de identificación** contemplados en esta Ley **como sistemas de firma** cuando permitan acreditar la autenticidad de la expresión de voluntad y consentimiento de los interesados → (firma no criptográfica)

[...] 5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.

Artículo 11. Uso de medios de identificación y firma en el procedimiento administrativo

[..] 2. Las AAPP **sólo** requerirán a los interesados el **uso obligatorio de firma** para:
a) Formular solicitudes
b) Presentar declaraciones responsables o comunicaciones
c) Interponer recursos
d) Desistir de acciones
e) Renunciar a derecho

5.2.3 Ley 40/2015: Firma de las AAPP

Artículo 42. Sistemas de firma para la actuación administrativa automatizada.

En el ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

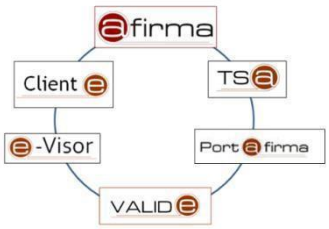
a) **Sello electrónico** de Administración Pública, órgano, organismo público o entidad de derecho público, **basado en certificado electrónico reconocido o cualificado** que reúna los requisitos exigidos por la legislación de firma electrónica.
b) **Código seguro de verificación (CSV)** vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Artículo 43. Firma electrónica del personal al servicio de las Administraciones Públicas.

b) 1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante **firma electrónica del titular del órgano o empleado público**. [...]

6. Servicios Comunes Firma Electrónica

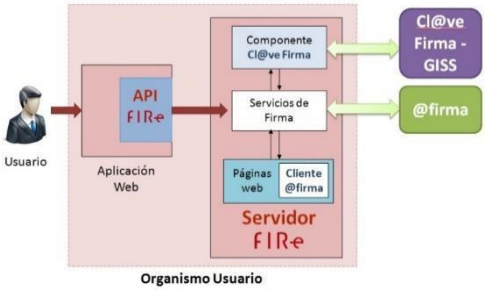
6.1 Suite @firma



- Plataforma @firma: permite la validación de certificados digitales mediante llamadas a WS
- Valide: permite la validación manual de firmas, certificados, y visualizar y realizar firmas
- TS@: permite realizar sellados y resellados de tiempo (firma longeva)
- Cliente @firma (Autofirma): permite la realización firmas en el cliente
- Cl@ve firma: permite la realización de firmas con certificado electrónico en la nube
- Integr@: facilita la integración con @firma y la realización de firma en servidor (sello del organismo) para entornos Java.

6.2 Fire

- FIRe es una solución que simplifica el uso y realización de firmas electrónicas de usuario al concentrar en un solo componente todos los requisitos de creación de firmas basadas tanto en certificados locales como en certificados en la nube.



Se recomienda revisar el tema de servicios comunes y su arquitectura en el Portal Administración Electrónica

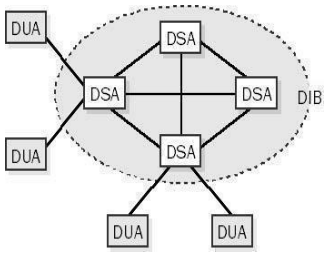
https://administracionelectronica.gob.es/ctt/fire/infoadicional#.WnA4b5fD40o

7. Servicios de Directorio

Un **servicio de directorio** es una aplicación que almacena de forma organizada **información sobre los usuarios de un sistema** y sobre el sistema en sí. A continuación, se analizan los protocolos de directorio X.500 y LDAP.

7.1 X.500

X.500 es el estándar de la ITU-T junto con la ISO (ISO/ IEC 9594) para servicio de directorio. Es muy flexible, aunque complejo.



Elementos de la arquitectura → **DIB** (Directory Information Base), **DSA** (Directory System Agent) y **DUA** (Directory User Agent).

La información de la DIB se almacena repartida entre los DSA.

Los DSA están organizados en dominios, existiendo réplicas de los datos en varios DSA de un mismo dominio.

Protocolos:

- DAP (Directory Access Protocol): DUA-DSA
- DSP (Directory System Protocol): DSA-DSA
- DISP (Directory Information Shadowing Protocol): DSA-DSA para réplicas de información
- DOP (Directory Operational Binding Management Protocol): para establecimiento de políticas entre DSAs

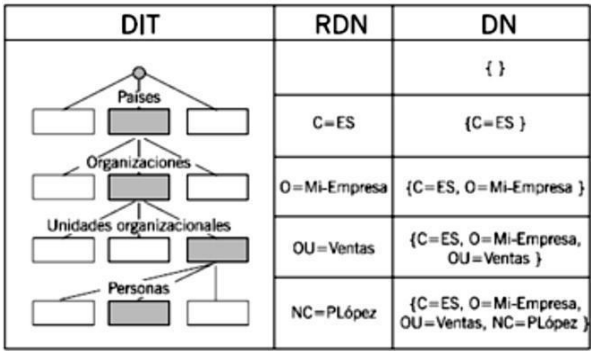
Modelo de información:

La información del directorio se organiza de forma **jerárquica en árbol** y se almacena como objetos atributo-valor en ASN.1

Modelo de direccionamiento:

Las entradas del árbol pueden identificarse de diferentes modos:

- **RDN** (Relative Distinguish Name)
→ Nombre de cada nivel del árbol
- **DN** (Distinguish Name)
→ Nombre completo y único de cada entrada del árbol.



7.2 LDAP (Lightweight Directory Access Protocol)

LDAP es un protocolo de nivel aplicación, estándar de IETF (RFC 2251 y RFC 2256) y abierto **para acceso a directorios** X.500 que pretende proveer un lugar centralizado para almacenar usuarios y credenciales.

- Es sólo el protocolo entre usuario y servidor, pero nombra a toda la solución.
- Versión actual: **LDAPv3 RFC 4511**
- Versión simplificada del DAP de X.500 usando TCP/IP puerto **389**; LDAPS (sobre SSL) puerto **636**.
- Compatible con X.500 y con funcionalidades similares, también definido en ASN.1, binario.

Modelo de información:

Emplea el **mismo modelo de X.500** basado en estructura jerárquica en árbol con objetos atributo-valor.

Modelo de direccionamiento:

Además de los direccionamientos mediante DN y RDN permite también el uso de **alias y registros referenciales (***referrals***).**

Modelo funcional:

Contempla las siguientes operaciones: **consulta** (search y compare), **modificación** (add, delete, rename, modify y modify_distinguished_name) y **autenticación y control** (bind, unbind y abandon)

Modelo de seguridad:

Contempla diferentes modos: anónima, autenticada y cifrada

7.3 LDIF (LDAP Data Interchange Format)

- Formato utilizado para el intercambio de datos en ficheros entre servidores LDAP de forma estandarizada
- Permite al cliente intercambiar datos con el servidor en formato ASCII (en vez de ASN.1). En caso de objetos no-texto (certificados, multimedia, etc.) se codificará en Base64 para pasarlo a texto.
- También se usa para exportación.
- También se puede usar para realizar actualizaciones y borrar entradas del directorio.

8. Otros servicios: Firma no criptográfica

Las condiciones para realizar firma no criptográfica se recogen en la ***Resolución de 14 de julio de 2017***, *de la Secretaría General de Administración Digital, por la que se establecen las* ***condiciones de uso de firma electrónica no criptográfica****, en las* ***relaciones*** *de los* ***interesados*** *con los* ***órganos administrativos*** *de la Administración General del Estado y sus organismos públicos*.

Debe garantizar igualmente la autenticidad, integridad y no repudio y dejar constancia de la voluntad del interesado. Será necesario:

- Utilizar un sello electrónico cualificado del organismo al que se añadirá un sello de tiempo (garantizar integridad).
- Garantizar la autenticidad del firmante autenticándose con Cl@ve
- Recoger evidencias para la verificación de identidad y esas evidencias también estarán selladas.
- Se devolverá un justificante con CSV verificable en sede.
- Incluir un campo de check con el que el interesado exprese su consentimiento y voluntad de firma.

La modificación a esta Resolución por la **Resolución del 20 de Octubre de 2022** persigue flexibilizar estas condiciones, permitiendo la autenticación con Cl@ve, sin restringirla a ningún nivel de calidad en la autenticación (básico, sustancial o alto).

Conforme al ENS, se podrán utilizar estos sistemas de firma no criptográfica, cuando el sistema de información haya sido categorizado de categoría **básica** y aquellos de **categoría media en los que no** sea necesario utilizar la **firma electrónica avanzada**, cuando así lo disponga la normativa reguladora aplicable.