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	**14/10/2024**

1. Identificación y firma electrónica

Firma electrónica: definición por Reglamento UE 910/2014 (eIDAS): el "*los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar*". **Concepto jurídico,** 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". **Concepto tecnológico**, (*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. La firma digital no garantiza la confidencialidad.

Modos de firma por múltiples firmantes:

- Cofirma: firma en paralelo
- Contrafirma (refrendo de firma): firma en cascada

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.

Los sistemas de **clave concertada** se aceptan como sistema de identificación en el **Art.9 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.

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. Para definirlos se utiliza el **estándar X.509 v3** (estándar de la ITU-T para infraestructuras de clave pública), que utilizan el lenguaje ASN.1

Para **validar** una firma digital no basta con validar la firma en sí, sino que, además es necesario validar el certificado asociado. 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 temporalmente suspendido antes de vencer el periodo de validez.

Se suele validar utilizando listas de revocación de certificados (CRL - *Certificate Revocation List*) mantenidas por las autoridades de certificación (CA), contienen **certificados revocados** (antes de su expiración) y la **fecha de revocación;** o bien validación por OCSP (*Online Certificate Status Protocol*) mediante el que se consulta directamente a la Autoridad de Validación (VA) sobre el estado del certificado.

***Sellos de tiempo*:** 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.

***Marca de tiempo*:** referencia temporal asociada a un documento.

1.1 Formatos de firma

- ***PKCS#7 / CMS*** *(Cryptographic Message Syntax)*. Permite diferentes tipos de objetos: data, signed-data, enveloped-data, signed-and-enveloped- data, digested-data y encrypted-data.
- ***CAdES*** *(CMS Advanced Electronic Signature)*

  Permite tanto *attached signature*, como *detached signature*.

  Define diferentes perfiles de datos firmados con CMS para firma electrónica avanzada:
  - **B-Level**: Firma con un formato básico.
  - **T-Level:** Añade sello de tiempos de la firma.
  - **LT-Level:** Añadiendo referencias a datos de verificación (certificados y listas de revocación).
  - **LTA-Level:** Archivado, añadiendo la posibilidad de re-sellado de tiempo periódico del documento archivado para prevenir el compromiso causado por la debilidad de los algoritmos de firma con el tiempo.
- **XMLDsig**
- ***XAdES*** *(XML Advanced Electronic Signature)*. Define varios perfiles de uso de XMLDsig para firma electrónica avanzada: XAdES B-Level, XAdES T-Level, XAdES LT-Level, XAdES LTA-Level
- ***PAdES*** *(PDF Advanced Electronic Signature)*
- ***S/MIME*** *(Secure / Multipurpose Internet Mail Extensions)*
- **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.

Cuando un certificado caduca, 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@).

1.2 Definiciones

- ***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*
  - *Estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable*

  (Definición referida al Reglamento eIDAS 910/2014)

- ***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* (Definición referida al Reglamento eIDAS 910/2014)
  Definiciones análogas para sello electrónico avanzado y cualificado *(para personas jurídicas)*

- ***Firma no criptográfica:*** Debe garantizar igualmente la autenticidad, integridad y no repudio y dejar constancia de la voluntad del interesado. El sistema se basa en la captura y almacenamiento de las evidencias relativas a la identificación, que debe realizarse mediante la plataforma Cl@ve, y aplica a todos los niveles de registro. ***Resolución del 20 de octubre de 2022, por la que se modifica la Resolución de 14 de julio de 2017****, de la SGAD, 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.*

- **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.
  (Definición referida al reglamento eIDAS 2.0 2024/1183).

2. Marco Regulatorio

- **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
- **Reglamento eIDAS 910/2014.**
- **Decisión de ejecución (UE) 2015/1506**: formatos reconocidos.
- **Reglamento eIDAS 2.0 UE 2024/1183.**
- **Ley 6/2020**, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- **Orden ETD/743/2022, de 26 de julio, por la que se modifica la 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.

3. 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. Los más usados son LDAP y X.500.

- X.500 es el estándar de la ITU-T junto con la ISO (ISO/ IEC 9594) para servicio de directorio.

  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.