# TEMA 081

# IDENTIFICACIÓN Y FIRMA ELECTRÓNICA (2) PRESTACIÓN DE SERVICIOS PÚBLICOS Y PRIVADOS. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI). MECANISMOS DE IDENTIFICACIÓN Y FIRMA: «SMART CARDS», DNI ELECTRÓNICO, MECANISMOS BIOMÉTRICOS

| | |
|---|---|
| **Versión** | **30.1** |
| **Fecha de actualización** | **08/09/2024** |

# ÍNDICE

# 1. Prestación de servicios públicos y privados

**Servicio de confianza:** servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

a) 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

b) 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

c) la **creación de firmas electrónicas o sellos electrónicos**

d) la **validación de firmas electrónicas o sellos electrónicos**

e) la **conservación de firmas electrónicas, sellos electrónicos, certificados** de firma electrónica o certificados de sello electrónico

**f)** la **gestión de dispositivos de creación de firma electrónica a distancia o dispositivos de creación de sello electrónico a distancia**

g) la **expedición de declaraciones electrónicas de atributos**

h) la **validación de declaraciones electrónicas de atributos**

i) la **creación de sellos de tiempo electrónicos**

j) la **validación de sellos de tiempo electrónicos**

k) la **prestación de servicios de entrega electrónica certificada**

l) la **validación de los datos transmitidos a través de servicios de entrega electrónica certificada** y las pruebas correspondientes

m) el **archivo electrónico** de datos y documentos electrónicos

n) la actividad de **registro de datos electrónicos en un libro mayor electrónico**

**Servicio de confianza cualificado:** servicio de confianza que cumple los requisitos aplicables del eIDAS.

**Prestador de servicios de confianza** (TSP, Trusted Service Provider): persona **física o jurídica** que presta uno o más servicios de confianza, bien como prestador **cualificado** o como prestador **no cualificado** de servicios de confianza;

**Prestador cualificado de servicios de confianza** (QTSP, Qualified TSP): prestador de servicios de confianza que presta uno o varios **servicios de confianza cualificados** y al que el **organismo de supervisión ha concedido la cualificación;**

El **Ministerio de Asuntos Económicos y Transformación Digital** actúa como **órgano de supervisión**, controlando el cumplimiento por los prestadores de **servicios** electrónicos de **confianza cualificados y no cualificados** conforme a Reglamento (UE) 910/2014 y Ley 6/2020.

- **Servicio de confianza cualificado**:
    1. Solicitud al órgano de supervisión junto con informe de evaluación de conformidad.
    2. El órgano de supervisión verificará si cumple los requisitos marcados en la normativa aplicable.
    3. Concesión o no concesión de la cualificación al prestador de servicios de confianza cualificado. En caso afirmativo, se actualizará la Lista de Confianza (TSL).

- **Servicio de confianza no cualificado:** pueden prestar servicios sin verificación previa de cumplimiento de requisitos, pero deberán comunicar al órgano supervisor la prestación del servicio en el plazo de 3 meses desde que inicien su actividad, a los meros efectos de conocer su existencia y posibilitar su supervisión.

Se pueden considerar prestadores públicos de servicios relacionados con la identificación:

- Prestadores de servicios de confianza públicos (incluidos en TSL):
  - autoridades de certificación (ej. Ministerio del Interior DGP)
  - autoridades de validación (ej. FNMT)
- Prestadores de servicios de identificación como Cl@ve.
- Red de nodos eIDAS.
- Las **Administraciones Públicas** están **obligadas** a **verificar la identidad** de los interesados en el procedimiento administrativo (Art. 9 Ley 39/2015).

Se pueden considerar prestadores privados de servicios:

- Prestadores de servicios de confianza privados (incluidos en TSL)
- Otras iniciativas privadas:
  - Red Alastria para la identificación digital basada en blockchain

Buscador de Prestadores de Servicios electrónicos de confianza:

https://sede.serviciosmin.gob.es/es-es/firmaelectronica/Paginas/Prestadores-de-servicios-electronicos-de-confianza.aspx

## 1.1 Reglamento (UE) Nº 910/2014 (eIDAS)

***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 por la que se deroga la Directiva 1999/93/CE.*

A destacar:

- **Artículo 2: Ámbito de aplicación**
  - El Reglamento se aplica a los **sistemas de identificación electrónica** notificados por los Estados miembros, a las **carteras europeas de identidad digital** proporcionadas por los Estados miembros y a los **prestadores de servicios de confianza** establecidos en la Unión. **NO** se aplica a la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes.
- **Artículo 3: Definiciones**
  - **Organismo de Evaluación de Conformidad:** organismo de evaluación de la conformidad definido en el artículo 2, punto 13, del Reglamento (CE) 765/2008, cuya competencia para realizar

una evaluación de la conformidad de un prestador cualificado de servicios de confianza y de los servicios de confianza cualificados que este presta, o cuya competencia para certificar carteras europeas de identidad digital o medios de identificación electrónica, esté acreditada en virtud de dicho Reglamento.

- **Identificación electrónica:** proceso consistente en utilizar los datos de identificación de la persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a otra persona física o a una persona jurídica.
- **Medios de identificación electrónica:** unidad material yo inmaterial que contiene los datos de identificación de la persona y que se utiliza para la autenticación en servicios en línea o, cuando proceda, en servicios fuera de línea.
- **Datos de identificación de la persona:** conjunto de datos que se emite de conformidad con el Derecho de la Unión o nacional y permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a otra persona física o a una persona jurídica.
- **Sistema de identificación electrónica:** régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a personas físicas o jurídicas o a personas físicas que representan a otras personas físicas o personas jurídicas.
- **Autenticación:** proceso electrónico que permite la confirmación de la identificación electrónica de una persona física o jurídica, o la confirmación del origen y la integridad de datos en formato electrónico.

### 1.1.1 Prestación de servicios de confianza

- **Artículo 19: requisitos de seguridad aplicables a los TSP** (completado con Art. 13 Ley 6/2020)

  **Medidas de seguridad:**

  Los prestadores cualificados y no cualificados de servicios de confianza adoptarán las medidas **técnicas y organizativas** adecuadas para gestionar los **riesgos para la seguridad** de los servicios de confianza que prestan.[...]

  **Notificación de violaciones de seguridad o pérdidas de integridad:**

  - Los prestadores de servicios de confianza (cualificados y no cualificados), en un **plazo máximo de 24 horas** tras tener conocimiento de una violación de seguridad o pérdida de integridad:
    - Notificarán al **organismo de supervisión** y, en caso pertinente, a otros organismos relevantes como el **organismo nacional en materia de seguridad** o la **autoridad de protección de datos.**
    - Notificarán a la **persona física o jurídica a la que se ha prestado el servicio,** si la violación o pérdida de integridad puede afectarle.
  - El organismo de supervisión notificado:
    - Notificará a **ENISA** y a los **organismos de supervisión de otros Estados** miembros, si la violación afecta a dos o más Estados miembros.
    - Informará al público (o exigirá al prestador que lo haga), si considera que la violación reviste interés general.
    - Facilitará a **ENISA un resumen anual de notificaciones** de violaciones de seguridad recibidas.

### 1.1.2 Inicio de prestación de servicio cualificado y listas de confianza

**INICIO DE UN SERVICIO DE CONFIANZA CUALIFICADO (QTSP)**

- **Artículo 21:** Cuando los TSP sin cualificación tengan intención de iniciar la prestación de servicios cualificados:

  1) Presentarán al organismo de supervisión una **notificación de su intención** junto con un **informe de evaluación** de la conformidad expedido por un organismo de evaluación de conformidad.
  2) El **organismo de supervisión verificará** si el prestador de servicios de confianza y los servicios de confianza que presta cumplen los requisitos establecidos en el Reglamento.
  3) Si cumple los requisitos, el organismo de supervisión **concede la cualificación** y notifica para **actualizar las listas de confianza.**

  Los QTSP pueden comenzar a prestar el servicio cualificado una vez que la cualificación haya sido indicada en la lista de confianza.

**LISTAS DE CONFIANZA**

- **Artículo 22:** Cada Estado miembro establecerá, mantendrá y **publicará listas de confianza** con información relativa a los **prestadores cualificados** de servicios de confianza con respecto a los cuales sea responsable, junto con la información relacionada con los servicios de confianza cualificados prestados por ellos.
  - Las listas se establecerán y publicarán **firmadas o selladas electrónicamente**, en una forma apropiada para el **tratamiento automatizado**.
  - Los Estados miembros notificarán a la Comisión información sobre el organismo responsable de la lista, el lugar en que se publica y los certificados empleados.

**ORGANISMO DE SUPERVISIÓN**

- **Artículo 17** (completado con art. 14 ley 6/2020) Los Estados miembros designarán un organismo de supervisión establecido en su territorio y notificarán a la Comisión los nombres y direcciones de éstos.

  [...] 3. Las funciones del organismo de supervisión serán las siguientes:

  *a)* **supervisar a los prestadores cualificados** de servicios de confianza establecidos en el Estado miembro a fin de garantizar, mediante **actividades de supervisión previas y posteriores**, que dichos QTSP y los servicios de confianza cualificados prestados, cumplen los requisitos del Reglamento;

  *b)* adoptar medidas, en caso necesario, en relación con los **prestadores no cualificados** de servicios de confianza establecidos en el Estado miembro, mediante **actividades de supervisión posteriores**, **cuando reciba la información** de que dichos TSP, o los servicios de confianza prestados por ellos, **no cumplan** los requisitos establecidos del Reglamento.

**SUPERVISIÓN DE LOS PRESTADORES CUALIFICADOS**

- **Artículo 20: [...]1**. Los **QTSP serán auditados, al menos cada 24 meses**, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad. [...]

  Sin perjuicio de lo anterior, **el organismo de supervisión podrá en cualquier momento auditar** o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de conformidad de los QTSP, corriendo con los gastos dichos prestadores [...]

3. Cuando el **organismo de supervisión** requiera a un QTSP que corrija el incumplimiento de requisitos y éste no actúe en consecuencia, el organismo de supervisión **podrá retirar la cualificación** al prestador o al servicio

### 1.1.3 Requisitos para los prestadores de servicios de confianza

**REQUISITOS APLICABLES A LOS TSP CUALIFICADOS**

- **Artículo 24.2** (completado con art. 9 ley 6/2020): Los QTSP que prestan servicios de confianza cualificados:
  a) **informarán** al organismo de supervisión de cualquier **cambio en la prestación** del servicio [...] al menos **1 mes** antes de llevarlo a cabo, y con una antelación de al menos **3 meses** en caso de que tengan intención de **cesar** tales actividades;
  b) contarán con personal y subcontratistas, con **conocimientos especializados**, fiabilidad, experiencia, cualificaciones y formación necesarias
  c) mantendrán **recursos financieros** suficientes o **pólizas de seguros** de responsabilidad adecuadas
  d) **informarán**, de manera clara, comprensible y fácilmente accesible, en un **espacio públicamente accesible** y de forma **individual**, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización
  e) utilizarán **sistemas y productos fiables** que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustenten, en particular utilizando técnicas criptográficas adecuadas;
  f) utilizarán **sistemas fiables para almacenar los datos** que se les faciliten de forma verificable
  g) adoptarán medidas adecuadas contra la falsificación, el robo o la apropiación indebida de datos o contra la eliminación, alteración o bloqueo de dichos datos sin tener derecho a ello;
  h) **registrarán** y mantendrán toda la **información** pertinente referente a los **datos expedidos y recibidos**
  i) Contarán con políticas adecuadas y adoptarán las medidas que procedan para gestionar los riesgos jurídicos, empresariales, operativos y otros riesgos directos o indirectos para la prestación del servicio de confianza cualificado. Al menos contarán con:
     - procedimientos de registro en un servicio e incorporación a este,
     - controles administrativos o de procedimiento,
     - gestión e implantación de servicios;
  j) contarán con un **plan de cese actualizado**
  k) garantizarán un **tratamiento lícito** de los **datos personales**
  l) si expiden certificados cualificados, mantendrán una **base de datos de certificados**.

Los prestadores cualificados de servicios de confianza que **expidan certificados cualificados**:

- Proporcionarán a cualquier parte usuario información sobre el estado de validez o revocación de los certificados (de forma automatizada, fiable, gratuita y eficiente)
- Cuando decidan revocar un certificado, **registrarán su revocación** en su base de datos y **publicarán** el estado de revocación (en un plazo de **24 horas** después de la recepción de la solicitud). La revocación será efectiva inmediatamente después de su publicación.

- **Artículo 24.1.bis. Verificación de la identidad**

  La verificación de la identidad se llevará a cabo por el prestador cualificado de servicios de confianza, bien directamente o bien por medio de un tercero, mediante uno de los siguientes métodos o de una combinación de los mismos:

  - cartera europea de identidad digital o de un medio de identificación electrónica notificado que satisfaga los requisitos para nivel de seguridad alto;
  - certificado de una firma electrónica cualificada o de un sello electrónico cualificado
  - otros métodos de identificación que garanticen la identificación de la persona con un nivel alto de confianza, cuya conformidad será confirmada por un organismo de evaluación de la conformidad;
  - a través de la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con el Derecho nacional.

### 1.1.4 Identificación electrónica transfronteriza

- **Artículo 6: Reconocimiento mutuo**

  1. Cuando sea necesaria una identificación electrónica [...] **para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro**, se **reconocerá** [...] el medio de identificación electrónica **expedido en otro Estado miembro**, siempre que:

     a) este **medio de identificación** electrónica haya sido expedido en virtud de un sistema de identificación electrónica **incluido en la lista publicada por la Comisión** de conformidad con el artículo 9.

     b) el **nivel de seguridad** de este **medio de identificación** electrónica corresponda a un nivel de seguridad **igual o superior** al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad **sustancial o alto**;

     c) el organismo público en cuestión utilice un nivel de seguridad **sustancial o alto** en relación con el **acceso a ese servicio** en línea.

  Este reconocimiento se producirá a más tardar 12 meses después de que la Comisión publique la lista.

  2. Un **medio de identificación** electrónica expedido por un sistema de identificación electrónica incluido en la **lista publicada** por la Comisión [...] y que corresponda al nivel de **seguridad bajo podrá ser reconocido** por los órganos del sector público [...]

- **Artículo 7: Condiciones para la notificación de los sistemas de identificación electrónica**

  Un sistema de identificación electrónica podrá ser objeto de notificación con arreglo al artículo 9.1, si se cumplen la totalidad de las condiciones siguientes: [...]

  c) que tanto el **sistema de identificación** electrónica como los medios de identificación electrónicos en virtud expedidos cumplan los requisitos de al menos uno de los **niveles de seguridad previstos.**

  f) el Estado miembro que efectúa la notificación garantiza la **disponibilidad de la autenticación en línea** de manera que cualquier usuario establecido en el territorio de otro Estado miembro pueda confirmar los datos de identificación de la persona recibidos en formato electrónico → (**nodos eIDAS**).

- **Artículo 8: Niveles de seguridad de los sistemas de identificación electrónica**

  1. Un **sistema de identificación electrónica notificado** en virtud del artículo 9, apartado 1, **deberá especificar los niveles de seguridad** bajo, sustancial y alto para los medios de identificación electrónica expedidos en virtud del mismo.

  2. Los niveles de seguridad bajo, sustancial y alto cumplirán los siguientes criterios, respectivamente:

     a) **el nivel de seguridad bajo** se referirá a un medio de identificación electrónica, [...] que establece un **grado limitado de confianza** en la identidad pretendida o declarada de una persona [...] y cuyo objetivo es **reducir el riesgo de uso indebido o alteración** de la identidad.

     b) **el nivel de seguridad sustancial** se referirá a un medio de identificación electrónica, [...] que establece un **grado sustancial de confianza** en la identidad pretendida o declarada [...] y cuyo objetivo es **reducir sustancialmente el riesgo de uso indebido o alteración** de la identidad.

     c) **el nivel de seguridad alto** se referirá a un medio de identificación electrónica [...] que establece un **grado de confianza** en la identidad pretendida o declarada de una persona **superior** al medio de identificación electrónica con un nivel de seguridad **sustancial**, [...]cuyo objetivo es **evitar el uso indebido o alteración de la identidad.**

## 1.2 Reglamento (UE) 2024/1183 (eIDAS 2) - Marco europeo de identidad digital

**Reglamento (UE) 2024/1183** del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del **marco europeo de identidad digital**.

El nuevo reglamento establece un marco para una identidad digital europea basado en el Reglamento eIDAS, en virtud del cual los Estados miembros de la UE podrían notificar voluntariamente los sistemas nacionales de identificación electrónica que otros Estados miembros estuvieran obligados a reconocer. Si bien el reconocimiento de la identificación electrónica notificada pasó a ser obligatorio en 2018, no se exigía a los Estados Miembros que elaboraran una identificación electrónica nacional. Esto supuso la implementación de una superestructura de interoperabilidad que conectaba los diversos sistemas de identidad, que era propensa a problemas técnicos. Esto ha dado lugar a discrepancias entre los países y ha impedido la extensión a los servicios digitales privados.

El nuevo Reglamento aborda las deficiencias de eIDAS mejorando la eficacia del **marco** actual para **la identidad digital** y ampliando sus beneficios al sector privado. Los Estados miembros deberán ofrecer a los

ciudadanos y las empresas **carteras digitales** que vinculen sus identidades digitales nacionales con pruebas de otros **atributos** personales, como permisos de conducción, diplomas y cuentas bancarias.

Estas carteras podrán ser emitidas por autoridades públicas o entidades privadas reconocidas. El objetivo es proporcionar a los europeos un control total sobre sus datos al acceder a los servicios en línea, eliminando el intercambio innecesario de datos. Se ofrecerá a los ciudadanos y a los proveedores de servicios en línea una arquitectura técnica, un marco de referencia y unas normas comunes que favorezca la armonización, fomentando la confianza y la interoperabilidad.

### 1.2.1 Principales novedades

- La creación de la **Cartera de Identidad Digital** o **"EU Digital Identity Wallet (EUDI)"** que permitirá a los usuarios **almacenar y compartir atributos** elegidos sin revelar información personal innecesaria.
- Aumenta el **control** que tienen los usuarios **sobre sus datos** personales, creando una identificación digital oficial de la UE y de cada estado miembro.
- Se introducen nuevos tipos de credenciales, como las **credenciales verificables**. Estas permiten a los usuarios demostrar y compartir sus atributos elegidos (edad, titulación, permisos, score crediticio, etc.) sin revelar información personal innecesaria.
- Amplía el catálogo de los servicios que podrán prestarse por los proveedores de confianza en torno a la nueva cartera digital europea.
- Facilita la **interoperabilidad** entre países, permitiendo que las identidades digitales sean válidas en toda la UE.
- Extiende su ámbito de aplicación a nuevos sectores como salud, movilidad y educación. Además, las FinTech y otras entidades financieras deberán utilizarlo para identificar a sus clientes.
- Se han definido **nuevos niveles de seguridad**: se introduce un cuarto nivel de seguridad "muy alto" para las transacciones de alto riesgo.
- Se **amplía** el ámbito de aplicación de los **servicios de confianza** para incluir el registro de datos electrónicos en un libro mayor electrónico, la gestión de la firma electrónica a distancia y los dispositivos de creación o los dispositivos de creación remota de sellos electrónicos.

### 1.2.2 Definiciones

Con la actualización del reglamento, se incorporan nuevas definiciones:

- **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.
- **Atributo:** característica, cualidad, derecho o permiso de una persona física o jurídica o de un objeto.
- **Declaración electrónica de atributos:** declaración en formato electrónico que permite la autenticación de atributos.

- **Declaración electrónica cualificada de atributos**: declaración electrónica de atributos expedida por un prestador cualificado de servicios de confianza.
- **Declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este:** declaración electrónica de atributos expedida por un organismo del sector público que sea responsable de una fuente auténtica o por un organismo del sector público que sea designado por el Estado miembro para expedir dichas declaraciones de atributos en nombre de los organismos del sector público responsables de las fuentes auténticas.
- **Fuente auténtica:** repositorio o sistema, mantenido bajo la responsabilidad de un organismo del sector público o de una entidad privada, que contiene y proporciona atributos acerca de una persona física o jurídica, o de un objeto, y que se considera una fuente principal de dicha información, o que está reconocido como auténtico de conformidad con el Derecho de la Unión o nacional, incluidas las prácticas administrativas.
- **Archivo electrónico:** servicio que garantiza la recepción, el almacenamiento, la recuperación y la eliminación de datos electrónicos y documentos electrónicos para asegurar su durabilidad y legibilidad, así como para preservar su integridad, confidencialidad y prueba de origen durante todo el período de conservación.
- **Servicio cualificado de archivo electrónico**: servicio de archivo electrónico prestado por un prestador cualificado de servicios de confianza.
- **Etiqueta de confianza de la UE para la cartera de identidad digital;** indicación verificable, sencilla y reconocible formulada de manera clara, de que la cartera europea de identidad digital de que se trate se ha proporcionado de conformidad con el presente Reglamento;
- **Autenticación reforzada de usuario:** autenticación basada en la utilización de al menos dos factores de identificación de diferentes categorías, ya sea conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) o inherencia (algo que es el usuario), que son independientes —es decir, que la vulneración de uno no compromete la fiabilidad de los demás—, y concebida de manera que se proteja la confidencialidad de los datos de autenticación.
- **Libro mayor electrónico:** secuencia de registros electrónicos de datos que garantiza la integridad de dichos registros y la exactitud de su orden cronológico.
- **Libro mayor electrónico cualificado:** libro mayor electrónico proporcionado por un prestador cualificado de servicios de confianza.
- **Correspondencia de la identidad:** proceso por el cual se establece una correspondencia o vínculo entre los datos o medios de identificación electrónica y una cuenta existente perteneciente a esa misma persona.
- **Registro de datos**: datos electrónicos registrados con metadatos relacionados que respaldan el tratamiento de los datos.
- **Modo fuera de línea**: en lo que respecta al uso de las carteras europeas de identidad digital, interacción entre un usuario y un tercero que tiene lugar en una ubicación física utilizando tecnologías de proximidad inmediata, sin necesidad de que la cartera europea de identidad digital acceda a sistemas a distancia a través de redes de comunicaciones electrónicas a efectos de la interacción.

### 1.2.3 Cartera europea de identidad digital

EUDI (European Union Digital Identity) es el sistema propuesto para construir un modelo de documentación digital de identificación de los ciudadanos, residentes y empresas de Europa. Las características de esta nueva herramienta son:

- Será **expedido** por cada uno de los Estados miembros, siguiendo unas directrices y estándares comunes.
- Se trata de un **producto y servicio** que permite al usuario **almacenar** sus datos identificativos, sus credenciales y otros atributos conectados con su identidad.
- Podrá utilizarse tanto para la **identificación *online* como *offline*** de personas físicas y jurídicas, así como para acceder a todo tipo de **servicios públicos o privados**. Todo ello siempre de forma transparente y bajo el control de su titular, en el ámbito territorial de toda la Unión Europea.
- **Su uso será gratuito** para las personas físicas.
- El **emisor** de dicha «Cartera o Monedero de Identidad Digital Europea» **no podrá recopilar ninguna información sobre su uso**, con la única excepción de aquella que sea necesaria para prestar el servicio de identificación.
- Deberá ser **accesible** a personas con discapacidades.
- Será **válida en todos los Estados miembros** para acceder a **servicios públicos** que requieran identificación electrónica.
- También deberá ser **aceptada por proveedores de servicios privados** como medio de identificación online. Entre otros, la propuesta del nuevo eIDAS 2 menciona las áreas de transporte, energía, bancos y servicios financieros, seguridad social, salud, agua, servicios postales, infraestructura digital, educación o telecomunicaciones.
- Se permite el **uso transfronterizo** de las «Carteras de Identidad Digital Europea» emitidas por cualquier Estado miembro, para el acceso a servicios públicos *online* en cualquier otro país dentro de la UE, siempre que se cumplan los requisitos que indica el reglamento.

**Principales beneficios de las carteras de identidad digital de la UE**

a) **Ciudadanos y empresas:**

1. **Control de usuario:** Los ciudadanos tendrán el poder de elegir qué aspectos de su identidad y datos comparten con terceros, garantizando la privacidad y el control sobre la información personal.
2. **Amplia usabilidad:** Las carteras de identidad digital de la UE estarán disponibles en toda la UE para acceder a servicios digitales públicos y privados, haciendo que las interacciones en línea sean más fluidas y eficientes.
3. **Transparencia y seguridad:** las carteras digitales de la UE tendrán licencia de código abierto, lo que garantizará la transparencia y la seguridad. Los usuarios tendrán la seguridad de que sus datos se manejan de forma segura, con medidas establecidas para evitar el uso indebido o el seguimiento ilegal.
4. **Facilidad de uso:** Las carteras digitales ofrecerán una interfaz fácil de usar, lo que permitirá a las personas administrar fácilmente sus identidades digitales y acceder a los servicios. La creación de firmas electrónicas cualificadas para uso no profesional será gratuita y mejorará la accesibilidad.

5. **Incorporación suave:** Los ciudadanos podrán utilizar los sistemas nacionales de identificación electrónica para registrarse en las carteras digitales, garantizando una transición fluida a la gestión de la identidad digital.

**b) Gobiernos:**

1. **Mejora del acceso a los servicios digitales:** las carteras digitales pueden agilizar el proceso de verificación de identidad, facilitando a los ciudadanos el acceso a los servicios gubernamentales en línea e impulsando la adopción.
2. **Mejorar la prevención del fraude:** Al proporcionar un medio de identidad seguro y verificable, puede ayudar a reducir el robo de identidad y el fraude relacionado con los servicios gubernamentales.
3. **Mejora la seguridad:** Se mejorará la seguridad general de los datos de los ciudadanos y se reducirá el riesgo de infracciones.

**c) Proveedores de servicios digitales:**

1. **Mejorar la seguridad y la privacidad:** Las carteras digitales pueden reducir el riesgo asociado con la responsabilidad de los métodos de autenticación tradicionales.
2. **Reducir el coste de la autenticación:** Las digitales pueden reducir los costes asociados con los procesos de verificación de identidad simplificándolos y automatizándolos.
3. **Evitar depender de grandes plataformas competidoras:** Los proveedores de servicios tendrán que depender menos de los servicios de identidad con un uso poco claro de los datos de usuario obtenidos.

**d) Sociedad:**

1. **Aumento de las transacciones en línea:** Con una verificación más fácil y segura, las personas pueden estar más inclinadas a participar en transacciones en línea.
2. **Nuevas oportunidades de negocio:** La adopción carteras digitales puede estimular la innovación, lo que lleva a nuevos servicios y productos.
3. **Reasignación de recursos:** Los recursos dedicados anteriormente a los procesos de verificación manual pueden ser redirigidos a usos más productivos.
4. **Crecimiento económico:** En general, una mayor adopción de transacciones en línea, nuevas oportunidades de negocio y una mejor asignación de recursos pueden contribuir a la estabilidad y el crecimiento económico general.

### 1.2.4 Credenciales digitales

Las credenciales son piezas de información que contienen afirmaciones sobre una persona, en un formato digital, que permiten verificar la identidad, las cualidades y las habilidades de un individuo de forma rápida, segura y confiable, lo que permite al verificador confiar en la veracidad de la reclamación. Los emisores de credenciales son terceros (en su mayoría organizaciones) en los que confía el verificador. Por lo tanto, las credenciales pueden ayudar al sujeto de la reclamación a participar plenamente en la sociedad y la economía.

Las credenciales incluyen una variedad de información, como el nombre, el apellido, la fecha de nacimiento, la cualificación educativa, las cualificaciones profesionales, la experiencia laboral, etc. A diferencia de las credenciales tradicionales, las credenciales digitales se presentan en un formato digital, utilizando tecnologías como la criptografía, con el fin de garantizar la seguridad, validez y autenticidad de la información.

Como parte del Reglamento Europeo de Identidad Digital, las credenciales digitales se introducen de manera que las personas puedan demostrar declaraciones sobre sí mismas y sus relaciones con el anonimato (es decir, sin revelar datos identificativos). Debido a su capacidad para proporcionar información verificada de manera segura y privada, las credenciales verificables se están volviendo cada vez más populares como una herramienta de autenticación digital confiable y segura.

### 1.2.5 Declaración electrónica de atributos

Los Estados miembros garantizarán la adopción de medidas que permitan a los prestadores cualificados de servicios de confianza de declaraciones electrónicas de atributos verificar por medios electrónicos, a petición del usuario, la autenticidad de los atributos siguientes, cotejándolos con las fuentes auténticas pertinentes a escala nacional o a través de intermediarios designados reconocidos a escala nacional, de conformidad con el Derecho de la Unión o nacional y cuando tales atributos se basen en fuentes auténticas pertenecientes al sector público:

- dirección,
- edad,
- sexo,
- estado civil,
- composición familiar,
- nacionalidad o ciudadanía,
- cualificaciones, títulos y licencias académicos,
- cualificaciones, títulos y licencias profesionales,
- facultades y mandatos para representar a personas físicas o jurídicas,
- permisos y licencias públicos,
- en el caso de las personas jurídicas, datos financieros y sociales.».

### 1.2.6 Próximos pasos

El Reglamento (UE) 2024/1183 por el que se establece el Marco Europeo de Identidad Digital ha entrado en vigor. El marco exige a los Estados miembros que proporcionen carteras de identidad digital de la UE a los ciudadanos en un plazo de veinticuatro meses a partir de la adopción de los actos de ejecución, en las que se describan las especificaciones técnicas y la certificación. Estas leyes, que se adoptarán entre seis y doce meses después de la aprobación del Reglamento, se basarán en los requisitos y especificaciones desarrollados para la caja de herramientas de identidad digital de la UE y garantizarán la aplicación uniforme de las carteras digitales en toda Europa.

## 1.3 Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza

***Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Deroga la ley 59/2003.***

Esta ley **no realiza una regulación sistemática de los servicios electrónicos de confianza, que ya han sido legislados por el Reglamento (UE) 910/2014.** El **objetivo** es **complementar** el Reglamento (UE) 910/2014 en aquellos aspectos que este no ha armonizado y que se dejan al criterio de los Estados miembros.

Esta ley **deroga** la **Ley 59/2003, de firma electrónica**

A destacar:

- **Artículo 2: ámbito de aplicación**
    - Esta Ley se aplicará a los prestadores públicos y privados de servicios electrónicos de confianza establecidos en España. Así mismo, se aplicará a los prestadores residentes o domiciliados en otro Estado que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país.
- **Artículos 4-6: Certificados electrónicos**
    - **Vigencia y caducidad de certificados:**
        - Vigencia: no superior a **5 años.**
        - Caducidad: los certificados electrónicos se extinguen por caducidad a la expiración de su período de vigencia, o mediante revocación por los prestadores de servicios electrónicos de confianza.
    - **Revocación y suspensión:** Los prestadores de servicios electrónicos de confianza extinguirán la vigencia de los certificados electrónicos mediante revocación en los siguientes supuestos:
        - Solicitud formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web.
        - Violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero.
        - Resolución judicial o administrativa que lo ordene.
        - Fallecimiento del firmante; capacidad modificada judicialmente sobrevenida, total o parcial, del firmante; extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio o pérdida de control sobre el nombre de dominio en el supuesto de un certificado de autenticación de sitio web.
        - Terminación de la representación en los certificados electrónicos con atributo de representante. En este caso, tanto el representante como la persona o entidad representada están obligados a solicitar la revocación de la vigencia del certificado en cuanto se produzca la modificación o extinción de la citada relación de representación.
        - Cese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador de servicios de confianza.

- Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.
- En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.
- Cualquier otra causa lícita prevista en la declaración de prácticas del servicio de confianza.

- **Identidad y atributos de los titulares de certificados cualificados: La identidad del titular en los certificados cualificados se consignará de la siguiente forma:**
  - En el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca. Los números anteriores podrán sustituirse por otro código o número identificativo únicamente en caso de que el titular carezca de todos ellos por causa lícita, siempre que le identifique de forma unívoca y permanente en el tiempo.
  - En el supuesto de certificados de sello electrónico y de autenticación de sitio web expedidos a personas jurídicas, por su denominación o razón social y su número de identificación fiscal. En defecto de este, deberá indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.
  - Si los certificados admiten una relación de representación incluirán la identidad de la persona física o jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento, público si resulta exigible, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

- **Artículo 9: obligaciones de los TSP**
  - Publicar información veraz.
  - No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.
  - Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.
  - El período de tiempo durante el que deberán conservar la información relativa a los servicios prestados será de **15 años** desde la extinción del certificado o la finalización del servicio prestado.
  - Constituir un seguro de responsabilidad civil por importe mínimo de **1.500.000 euros**, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, **se añadirán 500.000 euros** más por cada tipo de servicio.
  - El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una **antelación** mínima de **dos meses.**
  - **Enviar el informe de evaluación de la conformidad al Ministerio de Asuntos Económicos y**

**Transformación Digital**

- **Artículo 14: organismo de supervisión**
  - A nivel nacional, el **Ministerio de Asuntos Económicos y Transformación Digital** es el **organismo de supervisión**, teniendo la competencia de supervisión de los TSP.

- **Artículos 18 y 19: infracciones y sanciones**
  - **Muy Graves:**
    - La comisión de una infracción grave en el plazo de dos años desde que hubiese sido sancionado por una infracción grave de la misma naturaleza.
    - La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación.
  - **Graves:**
    - La resistencia, obstrucción, excusa o negativa a la actuación inspectora.
    - Actuar en el mercado como prestador cualificado de servicios de confianza, ofrecer servicios de confianza como cualificados o utilizar la etiqueta de confianza «UE» sin haber obtenido la cualificación de los citados servicios.
    - Almacenar o copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web.
    - No proteger adecuadamente los datos de creación de firma, sello o autenticación de sitio web cuya gestión se le haya encomendado.
    - El incumplimiento de la obligación de notificación de incidentes.
    - La expedición de certificados cualificados sin realizar todas las comprobaciones previas.
    - La ausencia de adopción de medidas, o la adopción de medidas insuficientes, para la resolución de los incidentes de seguridad en los productos, redes y sistemas de información, en el plazo de **diez días** desde que se hubiesen producido.
    - No cumplir con las obligaciones de constatar la verdadera identidad del titular de un certificado electrónico y de conservar la documentación que la acredite, en caso de consignación de un pseudónimo.
    - No extinguir la vigencia de los certificados electrónicos.
    - La prestación de servicios cualificados careciendo del correspondiente seguro obligatorio.
  - **Leves:**
    - Publicar información no veraz.
    - No comunicar el inicio de actividad, su modificación o cese por los prestadores de servicios no cualificados.
    - El incumplimiento por los prestadores cualificados de servicios de confianza de su obligación de remitir un informe anual de actividad al Ministerio de Asuntos Económicos y Transformación Digital **antes del 1 de febrero de cada año**.
    - El incumplimiento del deber de comunicación.
    - La falta o deficiente presentación de información solicitada por parte del Ministerio.

- Sanciones:
  - Por la comisión de infracciones **muy graves**, una multa por importe de **150.001** hasta **300.000** euros.
  - Por la comisión de infracciones **graves**, una multa por importe de **50.001** hasta **150.000** euros.
  - Por la comisión de infracciones **leves**, una multa por importe de hasta **50.000** euros.

## 1.4 Orden ETD/465/2021, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados

**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**, de 26 de julio.

Determina las **condiciones** y **requisitos técnicos** de **verificación de la identidad a distancia** y, si procede, de 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**.

El sistema deberá incorporar los medios técnicos y organizativos necesarios para verificar la autenticidad, vigencia e integridad de los documentos de identificación utilizados, verificar la correspondencia del titular del documento con el solicitante que realiza el proceso, mediante tecnologías como el reconocimiento facial, y verificar que este es una persona viva que no está siendo suplantada; debiendo quedar todos estos requisitos acreditados, en los términos que establece el anexo F11 de la Guía de Seguridad de las TIC CCN-STIC-140 , del Centro Criptológico Nacional mediante la certificación del producto.

# 2. Infraestructura de clave pública (PKI)

***PKI (Public Key Infraestructure)*** es el conjunto de elementos hardware, software, procedimientos, políticas y personal que permiten crear, almacenar, distribuir y revocar certificados digitales de clave pública.

## 2.1 Tipos de PKI

### 2.1.1 PKI basadas en Autoridades de Certificación

Existen autoridades de certificación que actúan como terceras partes de confianza creando los certificados X.509 que confirman la identidad de una persona y su clave pública asociada:

- Los certificados están firmados por una autoridad de certificación.
- La infraestructura basada en el estándar X.509 garantiza un **círculo de confianza**:
    - **Autoridad de certificación**: actúa como tercera parte de confianza garantizando la **autenticidad** de la persona identificada. Además, emite, gestiona y revoca los certificados electrónicos.
        - Las garantías y servicios que ofrecen se encuentran en la Declaración de Prácticas de Certificación.
        - Tienen Política de Certificación donde se observan los requisitos de emisión de certificados.
        - Se estructura en modo jerárquico:
            - CA root: certificado autofirmado de la raíz
                - CA subordinadas: firman con sus claves privadas los certificados electrónicos finales que emiten.

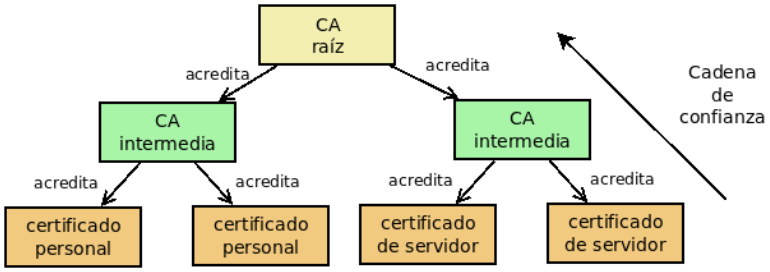


*Imagen 1: Estructura de la Autoridades de certificación en PKIs basadas en las mismas*

- **Autoridad de Registro: verifica la identidad del titular:**
    - Por comparecencia.
    - Remótamente.
    - Por medio de certificados cualificados de firma o sello
    - Como ejemplo, una autoridad de registro de la FNMT son las oficinas de atención al ciudadano.
- **Autoridad de validación: valida** los certificados mediante CRL u OCSP
- **Proveedores de Autoridad de certificación:**
    - Safelayer.
    - Entrust.
    - Microsoft Active Directory Certificate Services.

### 2.1.2 PKI basadas en redes de confianza

La confianza en los certificados se asigna de forma **descentralizada**, siendo los propios usuarios los que otorgan la confianza a las claves en función del conocimiento de su origen y la confianza que les merezcan los firmantes de los certificados.

- Los certificados están firmados por uno o más usuarios que atestiguan la identidad.

- Grados de confianza:
  - **Untrusted:** los certificados firmados con esa clave son ignorados.
  - **Marginal:** se necesitan dos claves marginales para firmar con validez a una tercera clave.
  - **Complete:** una sola clave puede firmar otra con validez.
  - **Ultimate:** se posee la clave privada y todas las que se firman son válidas.
- No se utiliza en las Administraciones Públicas.

### 2.1.3 Comparativa tipos de PKI

| | PKI X.509 | PKI Red de Confianza |
|---|---|---|
| **Firma de certificados** | CA | Autofirmado |
| **Confianza** | Centralizada en CA | Descentralizada |
| **Revocación** | Por la CA | Por el usuario |
| **Uso en AAPP** | Sí | No |

## 2.2 Estándares y tecnologías de la información utilizados en las PKIs

**X.509 v3** es el estándar de la ITU-T para infraestructuras de clave pública (ver tema 080).

**XKMS (XML Key Management Specification)** (Especificación XML para manejo de claves) es una especificación de W3C para la implementación de una PKI, permitiendo, mediante servicios web, el registro y distribución de claves públicas. Consta de dos partes:

- **XKRSS** – XML Key Registration Service Specification → registro, revocación y recuperación de claves públicas.
- **XKISS** – XML Key Registration Service Specification → obtención y validación de claves públicas.

# 3. Mecanismos de identificación y firma

## 3.1 Mecanismos de identificación y control de acceso

En general, el **control de acceso** consta de tres procesos (AAA):

- **Autenticación:** verificación de la identidad del usuario que solicita el acceso al recurso
- **Autorización:** proceso por el cual se determinan y restringen las acciones permitidas al usuario autenticado

Existen diferentes políticas de control de acceso:

- DAC (Discretionary Access Control)
- MAC (Mandatory Access Control)
- RBAC (Rol Based Access Control)

- **Trazabilidad:** monitorización y registro de los permisos concedidos y los recursos accedidos

Los métodos de autenticación son los métodos empleados para verificar la identidad de una entidad. Pueden estar basados en diferentes **factores de autenticación,** considerándose sistema de **autenticación fuerte** a aquel que emplea **al menos dos factores**:

- **Factor de conocimiento:** algo que el usuario sabe (ej. PIN)
- **Factor de posesión:** algo que el usuario tiene (ej. Token, móvil, etc)
- **Factor de inherencia:** algo que el usuario es (ej. Características biométricas)
- **Factor de conducta:** algo que el usuario suele hacer

A continuación, se analizan diferentes **mecanismos de autenticación**:

- **Contraseñas**
  - Se trata de información secreta y compartida (factor de conocimiento)
  - Pueden ser vulnerables a ataques de fuerza bruta contra el acceso o fuerza bruta contra el fichero de contraseñas.
  - Para evitar el problema de ataques de fuerza bruta contra el fichero de contraseñas por medio de diccionarios, se recomienda almacenar las contraseñas como *hash con sal*.
  - El uso de OTP (*one-time-password*) dificulta ataques y evita ataques de repetición.
- **Certificados digitales**
  - El mecanismo de autenticación se basa en demostrar que se posee la clave privada (factor de posesión).
  - El uso del certificado puede estar protegido por medio de contraseñas, por lo que se obtiene autenticación fuerte (factor de posesión y conocimiento).
- **Tarjetas inteligentes**
- **Mecanismos biométricos**

## 3.2 «Smart cards»

- Las tarjetas inteligentes o smartcards son chips criptográficos que pueden realizar tareas de autenticación y firma electrónica sin necesidad de que la clave privada salga del dispositivo.
- La norma ISO 7816 estandariza las tarjetas con circuito integrado.

- Clasificación según su **capacidad**:
    - **Tarjeta de memoria**: solo con capacidad de almacenamiento de información. Su aplicación fundamental es la identificación y control de acceso. Mantiene su contenido sin necesidad de energía externa. La memoria puede ser EPROM o EEPROM.
    - **Tarjeta microprocesadora:** contiene ficheros y aplicaciones. Pueden ser RAM, ROM, EPROM...
    - **Tarjeta criptográfica:** ejecutan operaciones de criptografía para realizar firma electrónica. Capaces de albergar claves privadas y certificados.
- Clasificación según su **conectividad**:
    - **Tarjetas de contacto**: deben ser insertadas en un lector para poder leer el chip (similar al chip de la SIM, aunque programados de manera diferente).
    - **Tarjetas sin contacto (contactless**): se comunican por radiofrecuencia, mediante RFID. Tienen un alcance de hasta 10cm.
    - **Tarjetas híbridas**: llevan 2 chips, uno con contacto y otro sin contacto.
    - **Tarjeta dual**: lleva 1 chip, pero presenta las interfaces de sin contacto y con contacto.
- Clasificación en función del **tamaño**:
    - **Tarjetas SIM:**
        - SIM estándar ISO/IEC 7810, ID-1, 1FF.
        - Mini-SIM: ISO/IEC 7810, ID-000, 2FF.
        - Micro-SIM: ETSI TS 102 221, Mini UICC, 3FF.
        - Nano-SIM: ETSI TS 102 221, 4FF.

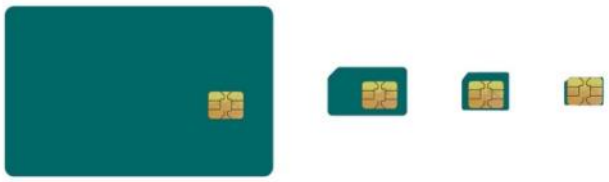

*Imagen 2: Tamaño de las tarjetas SIM.*

## 3.3 Mecanismos de firma

Existen diversos mecanismos de firma digital, algunos de los cuales son también empleados como mecanismos de identificación, como se ha visto anteriormente:

- **PADS**:
    - Dispositivos para captura digital de firmas realizadas manualmente por los usuarios. Típicos en comercios, mensajería, etc.
- **Certificados digitales almacenados en soporte software:**
    - Aquellos que se almacenan en la estructura de certificados en un ordenador, Tablet, smartphone y están disponibles en el dispositivo como mecanismos de ID y firma.

- **Tokens criptográficos** → 2 tipos (OTP, USB). Ambos tanto en soporte hardware como software.
    - **Generador OTP** (*One Time Password*) → contraseñas de un solo uso. Muy usados para acceso a intranet desde internet
    - **USB** → Almacenan contraseñas, certificados e identidad digital. En vez de memoria tiene un chip de seguridad con capacidad de operaciones cripto y *driverless* para mayor facilidad de uso.
- **Tarjetas criptográficas:** por ej. el DNIe.
- **HSM (Hardware Security Module):**
    - Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.
    - Puede ser empleado para realizar firmas remotas o firmas en la nube.
    - Ejemplo: en la AGE, CLAVE FIRMA (http://clave.gob.es/clave_Home/dnin.html) se soporta en equipos HSM.

## 3.4 DNI electrónico

El DNI electrónico permite **acreditar electrónicamente la identidad** de una persona, así como **firmar electrónicamente** documentos electrónicos, otorgándoles una validez jurídica equivalente a la de la firma manuscrita. (¡No permite cifrado de datos del usuario!)

Electrónicamente permite:

- Acreditar de forma indubitada la ID (*KU=DigitalSignature*) ➔ La identidad nunca es electrónica sino ID física acreditada por medios electrónicos.
- Firmar digitalmente documentos electrónicos (*KU=NonRepudiation/ContentCommitment*), jurídicamente equivale a firma manuscrita.

***Marco jurídico del DNI electrónico***:

- **Reglamento eIDAS 910/2014**: el certificado de firma del DNI es un certificado cualificado de firma electrónica, emitido por un prestador de servicios de confianza (Dirección General de la Policía) y está incluido en la TSL española. Recientemente modificado por la directiva 2022/2555 (NIS2, los cambios no están aún en vigor).
- **Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas**: en referencia a la identificación electrónica, la identificación con el DNIe proporciona un sistema basado en certificado electrónico cualificado de firma electrónica expedido por un prestador incluido en la TSL, como reconoce el art. 9. Respecto a la firma electrónica realizada con el DNIe es un sistema de firma electrónica cualificada basado en certificados electrónicos cualificados de firma electrónica expedido por prestador incluido en la TSL, como reconoce el artículo 10.
- **Ley 6/2020**: en la disposición adicional tercera se indica que permite acreditar electrónicamente la identidad personal. Se reconoce la eficacia del DNI para acreditar la identidad para todas las personas. (Normativa que le precede: **Ley 59/2003** de firma electrónica)
- **Real Decreto 1553/2005**, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica. En su artículo 12 se indica la validez de los certificados del DNI a 5 años. Se renuevan

en la misma tarjeta y con presencia física del titular. Si se pierde la validez del DNIe, también se pierde la validez de sus certificados.

- **Real Decreto 869/2013** por el que se regula la expedición del DNI y sus certificados.
- **Real Decreto 414/2015**, de 29 de mayo, por el que se modifica el Real Decreto 1553/2005
- **Reglamento 2019/1157** sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión. Se establece un formato común para los documentos de identidad de los países miembro. Implementado en el DNIe 4.0

***Estructura de PKI del DNI electrónico***:

En la PKI del DNI electrónico se han asignado las funciones de CA y VA a entidades diferentes:

- **Autoridad de Certificación**: Ministerio del Interior (Dirección General de la Policía)
- **Autoridad de Validación**: FNMT y MINHAC

***Certificados que contiene el DNIe***:

- Certificado cualificado de **autenticación** – claves RSA pública y privada de autenticación (*DigitalSignature*)
- Certificado cualificado de **firma** – claves RSA pública y privada de no repudio (*ContentCommitment*)
- Certificado cualificado de la **CA emisora** – clave pública de root CA para certificados *card-verifiables*

***Características técnicas específicas del DNI 4.0*** → https://www.dnielectronico.es/PDFs/DNI_4.0.pdf

### 3.4.1 Aplicaciones y liberación de código del dnie

- http://zonatic.usatudni.es → Plataforma SW de fuentes abiertas (SFL) para desarrollo rápido y seguro de apps DNIe
- DNIe Droid → Proyecto para realizar firma y autenticación con el DNIe en un terminal Android. Usa el controlador Java para DNIe de MinHAP, INCIBE y Red.es, certificado con EAL1.
- Mi DNIe → app gratuita creada por INCIBE y basada en DNIe Droid para interactuar con el DNIe desde Android

INCIBE ha liberado el código fuente del proyecto DNIe Droid para que empresas y desarrolladores puedan crear nuevas aplicaciones y servicios que usen DNIe en Android.

### 3.4.2 Comparación entre el dnie v2, el dnie 3.0 y el dnie 4.0

| | **DNIe v2** | **DNIe 3.0** | **DNIe 4.0** |
|---|---|---|---|
| ***Interfaz*** | Interfaz de contacto (chip) | Dual (contacto y *contactless*) | Dual y App móvil (sincronizado) |
| ***Chip*** | ST19LW34 y ST19LW34A | SLE78CLFX408AP Infineon Tech. | SoC ARM Cortex M (32 bits) |
| ***SO*** | DNI v 1.13 | DNIev3.0 (comercial) // DNIev4.0 | DNIe v4.0 |
| ***Capacidad*** | 32 K | 8K RAM - 400K Flash | 8K RAM - 750K Flash |
| ***Antena*** | NO | NFC | NFC |
| ***RFID*** | NO | Chip RFID – ISO 14443 | Chip RFID – ISO 14443 |
| ***Criptografía*** | **NO AES** / 3DES-CBC 128b/ **SHA1 160b**/ RSA, PKCS#1 v1.5, Miller-Rabin primalidad | **SÍ AES** / 3DES-CBC 128b/ **SHA-256**/ RSA 1024, PKCS#1 v1.5, Miller-Rabin primalidad | **SÍ AES** / 3DES-CBC 128b/ **SHA-256**/ RSA 2048, PKCS#1 v1.5, Miller-Rabin primalidad |
| ***Cert. CCN (Evaluation Assurance Level)*** | EAL4+ (*Methodically Designed, Tested and Reviewed*) | EAL5+ (*Semi-formally Designed and Tested*) | EAL5+ |

### 3.4.3 Contenido del chip del dnie 4.0

| **Zona pública (accesible read-only sin restricciones)** | **Zona seguridad (read-only, sólo en puntos DGP)** |
|---|---|
| – Claves Diffie-Hellman.<br>– Certificado CA intermedia emisora.<br>– Certificado de Autenticación (Digital Signature).<br>– Certificado de Firma (No Repudio) *****<br>– Certificado de componente (Card Authentication) | – Datos de filiación e ID (mismos que en facial)<br>– Imagen de la fotografía<br>– Imagen de la firma manuscrita<br>– Datos biométricos |

Los Estándares que cumple el DNIe son:

- ISO 7816.
- ISO 14443.
- Estructura interna de ficheros según PKCS#15.
- Autenticación de la información intercambiada entre las dos partes; incorporación de checksum criptográfico de tipo MAC según ANSI X9.19 y DES.

- Protocolo de establecimiento de las claves de sesión basado en el esquema propuesto en ISO/IEC 9798.

## 3.5 Mecanismos biométricos

- **Tecnologías biométricas de comportamiento:** se basan en rasgos derivados de la acción de la persona como el reconocimiento de la firma manuscrita, el reconocimiento de voz o el reconocimiento de la escritura de teclado.
- **Tecnologías biométricas fisiológicas:** se basan en rasgos físicos del cuerpo humano como la huella dactilar, el reconocimiento facial, el reconocimiento de iris o el reconocimiento de la geometría de la mano.
- En función de que umbral se establezca, se obtiene una mayor o menor tasa de fraude o tasa de insulto:
    - Tasa de fraude (falso positivo o error de etiquetado)
    - Tasa de insulto (falso negativo o error de no etiquetado)
- Los principales usos de la biometría son:
    - Control de accesos.
    - Control de presencia.
    - Lucha contra el fraude.
    - Medios de pago…
- La **biometría cancelable** consiste en aplicar una transformación en las plantillas biométricas generadas por los sistemas para proporcionar seguridad y privacidad. Se utilizan funciones matemáticas complejas para transformar los datos originales (huella digital, cara, …) de modo irreversible, siendo imposible reconstruir a partir de los datos almacenados los datos originales.
- Las características deseables en los sistemas biométricos son: universalidad, capacidad de diferenciación, permanencia, accesibilidad y amigable.

## 3.6 Marco regulatorio aplicable a la identificación y firma electrónica en las AAPP

- **Ley 39/2015**: identificación de los interesados
    - **Artículo 9: Sistemas de identificación de los interesados en el procedimiento.**
        - Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

- Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:
  - Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.
  - Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.
  - Cualquier otro sistema que las Administraciones públicas consideren válido.
- En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.

- **Artículo 11: Uso de medios de identificación y firma en el procedimiento administrativo.**
  - Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.
  - Las Administraciones Públicas sólo **requerirán** a los interesados el uso obligatorio de firma para:
    - **Formular solicitudes.**
    - **Presentar declaraciones responsables o comunicaciones.**
    - **Interponer recursos.**
    - **Desistir de acciones.**
    - **Renunciar a derechos.**

- **Ley 40/2015**: identificación de las AAPP
  - **Artículo 38: La sede electrónica.**
    - La sede electrónica es aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.
    - El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.
    - Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del órgano titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.
    - Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.
    - La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso

generalizado por los ciudadanos.

- Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente.

- **Artículo 40: Sistemas de identificación de las Administraciones Públicas.**
  - Las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.
  - Se entenderá identificada la Administración Pública respecto de la información que se publique como propia en su portal de internet.

- **RD 311/2022**, Esquema Nacional de Seguridad
  - Medidas de seguridad de *Control de acceso (op.acc]*.
  - Medida de seguridad *Mecanismos de autenticación [op.acc.5 y op.acc.6]*.