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**

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**.

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**
    - **Sistemas de identificación electrónica** notificados por los Estados miembros
    - **Carteras europeas de identidad digital** proporcionadas por los Estados miembros
    - **Prestadores de servicios de confianza** establecidos en la Unión.

1.1.1 Prestación de servicios de confianza

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

  Notificación de violaciones de seguridad o pérdidas de integridad: prestadores de servicios de confianza (cualificados y no cualificados), en un **plazo máximo de 24 horas** , notificarán al **organismo de supervisión** y, si procede, al **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 afectados y facilitará **un resumen anual de notificaciones** de violaciones de seguridad recibidas.
        - Informará al público (o exigirá al prestador que lo haga),si se considera de interés general.

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.

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. [...]

1.1.2 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.
  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 **información** sobre el **estado de validez o revocación** de los certificados (automatizada, fiable, gratuita y eficiente)
- **registrarán su revocación** en su base de datos y **publicarán** el estado de revocación (**24 horas**)

- **Artículo 24.1.bis. Verificación de la identidad**
  - cartera europea de identidad digital o de un medio de identificación electrónica (nivel de seguridad alto)
  - certificado de una firma electrónica cualificada o de un sello electrónico cualificado
  - otros métodos de identificación aceptados por un organismo de evaluación de la conformidad;
  - presencia física de la persona física o de un representante autorizado de la persona jurídica.

1.1.3 Identificación electrónica transfronteriza

- **Artículo 6: Reconocimiento mutuo**
- **Artículo 8: Niveles de seguridad de los sistemas de identificación electrónica** (bajo, sustancial, alto)

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**.

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 y manteniendo el **control** que tienen los usuarios **sobre sus datos** personales.
- Nuevos tipos de credenciales, como las **credenciales verificables** que permiten a los usuarios demostrar y compartir sus atributos elegidos sin revelar información personal innecesaria.
- 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.
- 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**
- **Atributo**
- **Declaración electrónica de atributos**

- **Declaración electrónica cualificada de atributos**
- **Declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este**
- **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**
   2. **Amplia usabilidad**
   3. **Transparencia y seguridad**
   4. **Facilidad de uso**
   5. **Incorporación suave**

b) Gobiernos:
   1. **Mejora del acceso a los servicios digitales**
   2. **Mejorar la prevención del fraude**
   3. **Mejora la seguridad**

c) Proveedores de servicios digitales:
   1. **Mejorar la seguridad y la privacidad**
   2. **Reducir el coste de la autenticación**
   3. **Evitar depender de grandes plataformas competidoras**

d) Sociedad:
   1. **Aumento de las transacciones en línea**
   2. **Nuevas oportunidades de negocio**
   3. **Reasignación de recursos**
   4. **Crecimiento económico**

1.2.4 Próximos pasos

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.

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

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**
    - Prestadores públicos y privados de servicios electrónicos de confianza establecidos en España y 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: expiración de su período de vigencia, o mediante revocación
    - **Revocación y suspensión:** mediante
        - 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
        - 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.
        - Cese en la actividad del prestador de servicios de confianza salvo transferencia a otro prestador de servicios de confianza.
        - Descubrimiento de la falsedad o inexactitud de los datos aportados
        - 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.

- **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**
- **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

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**. Conforme al 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.

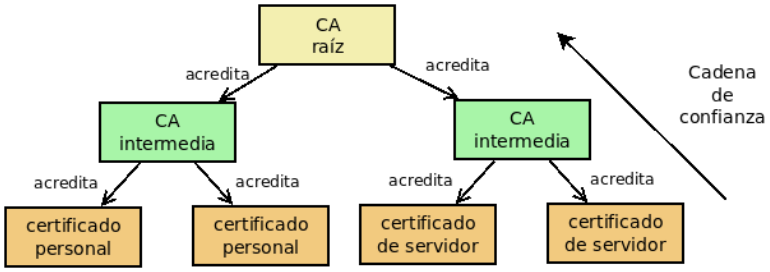

Imagen 1: Estructura de la Autoridades de certificación en PKIs basadas en las mismas

- **Autoridad de Registro: verifica la identidad del titular**
- **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**
- **Certificados digitales**
- **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.

3.3 Mecanismos de firma

- **PADS**: Dispositivos para captura digital de firmas realizadas manualmente por los usuarios. Típicos en comercios, mensajería, etc.
- **Certificados digitales almacenados en soporte software**
- **Tokens criptográficos** → 2 tipos (OTP, USB). Ambos tanto en soporte hardware como software.
- **Tarjetas criptográficas:** por ej. el DNIe.
- **HSM (Hardware Security Module):** dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

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!)

Marco jurídico del DNI electrónico:

- **Reglamento eIDAS 910/2014**
- **Ley 39/2015, Procedimiento Administrativo Común de las Administraciones Públicas**
- **Ley 6/2020**
- **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*

3.4.1 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+

3.4.2 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. – Certificado CA intermedia emisora. – Certificado de Autenticación (Digital Signature). – Certificado de Firma (No Repudio) ***** – Certificado de componente (Card Authentication)	– Datos de filiación e ID (mismos que en facial) – Imagen de la fotografía – Imagen de la firma manuscrita – 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.
- **Tecnologías biométricas fisiológicas:** se basan en rasgos físicos del cuerpo humano.
- 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)

- La **biometría cancelable** consiste en aplicar una transformación en las plantillas biométricas generadas por los sistemas para proporcionar seguridad y privacidad.
- 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.**
  - **Artículo 11: Uso de medios de identificación y firma en el procedimiento administrativo.**
- **Ley 40/2015**: identificación de las AAPP
  - **Artículo 38: La sede electrónica.**
  - **Artículo 40: Sistemas de identificación de las Administraciones Públicas.**

- **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]*.