# 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

Un **servicio de confianza** es un servicio electrónico consistente en la creación, verificación y validación de firmas electrónicas o sellos de tiempo; servicios de entrega electrónica certificada; preservación de firmas u otros.

El **prestador de servicios de confianza** (TSP, *Trusted Service Provider*) es la persona física o jurídica que presta un servicio de confianza, cumpliendo con los criterios para ello establecidos por las normas.

**Marco regulatorio aplicable a la identificación y firma electrónica en las aapp**

- **Reglamento 910/2014**: identificación en servicios públicos y reconocimiento mutuo de identidades
    - Artículo 2: ámbito de aplicación
    - Artículo 3: definiciones
    - Artículo 6: reconocimiento mutuo de medios de identificación
    - Artículo 7: notificación de sistemas de identificación
    - Artículo 8: Niveles de seguridad de los sistemas de identificación electrónica (bajo, sustancial, alto)
    - Artículo 19: requisitos de seguridad aplicables a los TSP
    - Artículo 20: supervisión de los prestadores cualificados de servicios de confianza
    - Artículo 21: inicio de un servicio de confianza cualificado
    - Artículo 22: listas de confianza
    - Artículo 24: requisitos para los prestadores cualificados de servicios de confianza
- **Reglamento 2024/1183:** modifica el Reglamento 910/2014 - Marco europeo de identidad digital.
    - **Cartera de Identidad Digital** o **"EU Digital Identity Wallet (EUDI)"** y declaración electrónica de atributos
    - **Credenciales verificables**
    - **Nuevos niveles de seguridad**
    - **Nuevos servicios de confianza** (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,...).
- **Ley 6/2020:** reguladora de determinados aspectos de los servicios electrónicos de confianza
    - Artículo 2: ámbito de aplicación
    - Artículos 4-6: Certificados electrónicos
    - Artículo 9: obligaciones de los TSP
    - Artículos 18 y 19: infracciones y sanciones
- **Orden ETD/465/2021**:métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados
- **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]*.

# 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.

En las PKIs basadas en autoridades de certificación se distinguen varios componentes:

- **Autoridad de certificación (CA**): es una tercera parte de confianza que expide, gestiona y revoca certificados digitales
  - Las CAs firman con su clave pública los certificados que expiden.
  - Los certificados de las propias CAs son públicos, para que los usuarios puedan así validar las firmas de los certificados expedidos por las CA.
  - Las CAs están organizadas de forma jerárquica, de manera que el certificado de una CA está firmado por una CA de nivel superior
  - Los CAs raíz firman sus propios certificados.

La clave de una CA es la más duradera en validez. Cuando la clave va a expirar, los certificados cuyo periodo de validez exceda el de la antigua clave, se refirmarán con la nueva clave.

- **Autoridad de registro (RA):** Auxilia a la CA en el proceso de verificar la identidad del titular que solicita la expedición de un certificado. Además, por delegación de las Cas, suelen encargarse también de recibir y procesar las solicitudes de revocación de certificados.

Ejemplos de RA: AEAT, Policía, SegSoc, SocEst Correos y Telégrafos.

**Funciones**:

- Publicación de certificados y de las CRLs de la CA
- Recibir solicitudes de revocación y renovación de certificados
- Generación de informes y de avisos de expiración de certificados.
- Identificar fehacientemente al firmante y **autorizar la emisión de su certificado**.

- **Autoridad de validación (VA**): validan el estado de los certificados mediante CRLs u OCSP
- **Directorio:** empleado por las CAs para el almacenamiento y distribución de certificados y CRLs
- **Proveedor de CA:** proveedores de las tecnologías de CA (ej. Safelayer, Entrust, EJBC, Microsoft)

# 3. Mecanismos de identificación y firma

- **Control de acceso** consta de tres procesos (AAA):
  - **Autenticación**
  - **Autorización**
  - **Trazabilidad**
- **Factores de autenticación:** sistema de **autenticación fuerte**, emplea **al menos 2 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
- **Mecanismos de autenticación**:
  - **Contraseñas**
  - **Certificados digitales**
  - **Tarjetas inteligentes o "Smart cards"**
  - **Mecanismos biométricos**
- **Mecanismos de firma:**
  - **PADS**
  - **Certificados digitales almacenados en soporte software**
  - **Tokens criptográficos** → 2 tipos (OTP, USB)
  - **Tarjetas criptográficas:** por ej. el DNIe.
  - **HSM (Hardware Security Module)**
- **DNI electrónico**
  - El DNI electrónico permite **acreditar electrónicamente la identidad** (*DigitalSignature*) de una persona, así como **firmar electrónicamente** documentos electrónicos (*KU=NonRepudiation/ContentCommitment*), otorgándoles una validez jurídica equivalente a la de la firma manuscrita. (¡No permite cifrado de datos del usuario!)
  - ***Estructura de PKI del DNI electrónico***: en la PKI del DNI electrónico se han asignado las funciones de CA y VA a entidades diferentes:
    - **CA**: Ministerio de Interior (Dirección General de la Policía)
    - **VA**: FNMT y MINHAC

| | **DNIe v2** | **DNIe 3.0** | **DNIe4.0** |
|---|---|---|---|
| ***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+ |

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 |