# Firma electrónica

# Presentación.

- Soy Andrés Ramírez (Andy, aoramire@dipalme.org, 1221), Jefe de la Sección de Bases de Datos y Coordinación dentro del Servicio de Nuevas Tecnologías.
- Mi equipo y yo no encargamos de:
  - Gestionar la bases de datos y documentos.
  - Gestionar sistemas de firma electrónica y port@firmas.
  - Gestionar servidores de aplicaciones.
  - Gestionar certificados de sello, de sitio y de sede.
  - Integraciones y otros procesos.

# Qué vamos a ver.

- Régimen jurídico de la firma electrónica.
- Usos.
- Tipos de firma conforme a la ley.
- Formatos de firma.
- Dispositivos y sistemas de firma.
- Certificado electrónico.
- Documento y expediente electrónico.

# Régimen jurídico.

- Conforme a https://firmaelectronica.gob.es/Home/Ciudadanos/Base-Legal.html
  - La firma electrónica se regula en nuestro ordenamiento jurídico mediante la aplicación de la **Ley 6/2020**, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el **Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo**, de 23 de julio de 2014 (eIDAS), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
  - Debemos destacar que la reciente Ley 6/2020 ha derogado la Ley 59/2003, de 19 de diciembre, de firma electrónica.

# Régimen jurídico: propósito.

- El propósito de la firma electrónica es:
  - Identificar al firmante de manera inequívoca.
  - Asegurar la integridad de lo firmado.
  - No repudio de lo firmado.

- Consecuencias derivadas:
  - Eliminación del papel.
  - Agilidad en la tramitación.

# Usos.

- Firma electrónica de documentos **digitales** (*).
- Notificación electrónica.
- Comunicación segura entre procesos de gestión y sistemas ~ **Administración Electrónica**.
- Firma de correos electrónicos y factura electrónica.
- Etc.

# Usos.

- Es importante que hago referencia a **documentos digitales** y no a **documentos electrónicos**.
- Un documento electrónico es un documento digital que posee un conjunto de metadatos que describen su contenido y características conforma a las especificaciones del Esquema Nacional de Interoperabilidad (ENI).
- Un documento electrónico puede estar firmado o no.

# Usos.

- La agregación de documentos electrónicos dentro de un expediente junto al conjunto de metadatos del expediente conforme al ENI es un expediente electrónico.
- El expediente electrónico es un paquete exportable e interoperable entre los sistemas de información que dan soporte a la Administración Electrónica.
- Ver página 43.

# Tipos de firma conforme a la ley.

- Los tipos de firma conforme a la ley son:
  - Firma electrónica simple.
  - Firma electrónica avanzada.
  - Firma electrónica cualificada o reconocida.

# Tipos de firma conforme a la ley: simple.

- **Firma electrónica simple**: datos electrónicos consignados a otros que permiten identificar al firmante.

  Ejemplo documento en un correo electrónico personal corporativo o con especificación de los datos personales del firmante.

# Tipos de firma conforme a la ley: avanzada.

- **Firma electrónica avanzada**: firma electrónica simple que:
  - Está vinculada al firmante de manera única y permite la identificación del firmante.
  - Ha sido creada utilizando elementos que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.
  - Está vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable. De esta necesidad surge lo que se denomina **huella o resumen criptográfico**.

# Tipos de firma conforme a la ley: avanzada: huella.

- **Huella**, **resumen** o **hash criptográfico** es el resultado de la aplicación de algoritmos matemáticos que relacionan un conjunto arbitrario de datos electrónicos de partida a una lista de datos resultado reducida de tamaño fijo.
- Estos algoritmos son de un solo sentido, es decir dado un conjunto de datos de partida siempre se obtiene la misma lista de datos resultado. Cualquier pequeña modificación de los datos de partida obtiene una lista de datos resultado diferente.
- Información: https://en.wikipedia.org/wiki/Cryptographic_hash_function

# Tipos de firma conforme a la ley: avanzada: huella.

- Los algoritmos más utilizados en la firma electrónica son:
  - MD5 (16 bytes, depreciado por vulnerabilidad en procesos de ingeniería inversa).
  - SHA-1 (20 bytes, depreciado por el mismo motivo).
  - SHA-2: concretamente SHA-256 (32 bytes) y SHA-512 (64 bytes).

# Tipos de firma conforme a la ley: cualificada.

- **Firma electrónica cualificada** o **reconocida**:

  es toda aquella firma electrónica avanzada que se ha creado con un **dispositivo cualificado** de creación de firmas electrónicas (ver página 29),

  y que se basa en un **certificado cualificado** de firma electrónica, es decir, un certificado de firma electrónica, que ha sido expedido por un **prestador cualificado de servicios de confianza**. (ver página 42).

# Qué es la firma electrónica cualificada.

- La firma electrónica es un conjunto de datos binarios que se **relacionan de forma inequívoca** con los datos de partida originales.
- Cualquier pequeña modificación en los datos de partida originales rompe esta relación y por tanto constata una **modificación posterior a la firma**.
- La firma puede estar contenida en un fichero aparte o en el mismo fichero de partida original, en función al **formato de firma**.
- Por motivos de rendimiento y espacio, no se firma el conjunto de datos de partida originales sino la **huella criptográfica** de los mismos (ver página 12).

# Qué es la firma electrónica cualificada: TSA.

- Normalmente es preciso asociar la firma electrónica al instante en el tiempo en que se produce.
  Así se puede dejar constancia de que la firma no se produjo ni antes ni después de ese momento, importante por ejemplo a la hora de presenta una solicitud de presentación a pruebas selectivas.
- El proceso de estampación de firma electrónica se le conoce como sellado de tiempo y es realizado por la **TSA** (ver página 42).

# Qué es la firma electrónica cualificada: TSA.

- La TSA es un sistema de confianza (FirmaProfesional, Gobierno de España, FNMT, Junta de Andalucía) que firma la firma realizada añadiéndole metadato del instante de tiempo.
- El metadato de firma es de tipo «`timestamp`» con formato «`año-mes-día-hora-minutos-segundos-milisegundos-zonahoraria`» en formato binario.
- El sellado de tiempo es una firma que la TSA realiza sobre la última firma (o conjunto de firmas) electrónica del documento.

# Formatos de firma.

- CMS.
- PDF signature.
- XML Signature.
- Firma por evidencias con Cl@ve.

# Formatos de firma: CMS.

- Precisa de dos ficheros:
  - Original con datos que se pretenden firmar.
  - Firma: fichero binario resultado de aplicar el algoritmo de firma y el certificado sobre la huella del fichero original.
- La firma por sí misma no contiene los datos firmados.
- Es preciso proveer los dos ficheros (original y firma).
- Es válido para cualquier tipo de fichero o dato.
- Dado el fichero «`FICHERO.EXT`» a firmar, la firma normalmente es «`FICHERO.EXT.csig`».

# Formatos de firma: CMS.

- Este formato de firma es válido para firmar cualquier tipo de fichero.
- No genera copias de los datos de partida originales y su codificación es binaria, por lo que ocupa poco espacio.
- Es el formato de firma por defecto en Diputación (excepto en la oficina virtual).

# Formatos de firma: PDF Signature.

- Dado un documento PDF la firma genera un nuevo fichero PDF que contiene inalterados los datos textuales del documento de partida original, al que se le añade el conjunto de datos de la firma.
- El fichero nuevo contiene toda la información: documento original y firma electrónica.
- Sólo es válido para documentos PDF y genera copia completa de contenido.
- Internamente la firma se almacena en la estructura del documento PDF usando el formato anterior CMS.

# Formatos de firma: XML Signature.

- Puede ser de dos tipos:
  - **Desacoplada**: igual que en CMS genera un fichero XML aparte que contiene únicamente la firma. Precisa del conjunto de datos originales.
  - **Acoplada**: igual que en PDF Signature, genera un nuevo fichero XML que contiene el conjunto de datos originales y la firma. No precisa del documento original.
- La codificación interna es en formato base-64 con lo que el tamaño resultado puede ser entre un 40% y un 60% superior al de partida original, mucho menos eficiente en espacio que CMS.
- La ventaja es la integración nativa con el mundo de los servicios web y servicios Rest.

# Formatos de firma: firma por evidencias.

- Entre los formatos de firma, se encuentra la llamada firma por evidencias con Cl@ve: https://clave.gob.es/clave_Home/dnin/queEs.html
- Esto no es una firma algorítmica al uso sino una procedimiento de reconocimiento legal de firma si:
  - Estar dado de alta en Cl@ve permanente.
  - Se realiza lo que denominan un doble factor de autenticación.
- Este formato de firma se utiliza en la oficina virtual de Diputación.

# Formatos de firma: firma por evidencias.

- Se considera que si el firmante se autentica para iniciar trámite, y por otro medio distinto de los ofrecidos por Cl@ve vuelve a autenticarse en el momento de la firma, Cl@ve toma el proceso como correcto de firma al haber identificado correctamente al firmante, y realiza una firma con certificado de sello de las evidencias de la doble autenticación y le añade un sello de tiempo.
- Como resultado es devuelto un mensaje SAML con toda la información de la firma. Esta es firmada ya en la oficina virtual con nuestro certificado de sello.
- Ventaja: no precisa de certificados de usuario.

# Formatos de firma electrónica avanzados.

- Son conocidos como:
  - CAdES para CMS.
  - PAdES para PDF Signature.
  - XAdES para XML Signature.
- De ahora en adelante serán especificados como AdES para englobar a CAdES, PAdES y XadES a la vez.

# Formatos de firma electrónica avanzados.

- Los distintos niveles AdES, desde menos informado a más informado son:
  - **AdES-BES**: firma cualificada que cumple con la Ley respecto a las directivas de firma electrónica avanzada (ver página 11).
  - **AdES-EPES**: es AdES-BES con información adicional sobre política de firma, certificado empleado para la firma y CA que lo emitió.
  - **AdES-T**: es AdES-EPES con sellado de tiempo de una TSA cualificada (ver página 16).
  - **AdES-C**: es AdES-T con información sobre estado de no revocación resultado de las consultas a los servicios OCSP o CRL correspondientes (ver página 39).

# Formatos de firma electrónica avanzados.

- **AdES-X**: es AdES-C con información del instante de las consultas de AdES-C.
- **AdES-XL**: es AdES-X con clave pública de los certificados implicados en la firma y sellado de tiempo. Ocupa mucho por añadir las claves públicas.
- **AdES-A**: es AdES-X con información de políticas de refirmado para hacer la firma perdurable en el tiempo.

La política de firma es una norma que especifica los tipos y formatos de firma válidos, regulación y procesos de validación y refirmado.

# Formatos de firma electrónica avanzados.

- El refirmado es un proceso que consiste en asegurar fortaleza del algoritmo de firma mediante la aplicación sobre la última firma (o conjunto de firmas) de nuevos algoritmos de firma más modernos o claves de certificados más largas.

  El refirmado normalmente es un resellado de tiempo por la TSA, o refirmado con el certificado de sello de entidad.

- Burbuja → ordenadores cuánticos → algoritmo de Peter Shor → Distopía.

# Dispositivos seguros de firma electrónica.

- En Diputación de Almería:
  - @Firma, modelo federado y modelo nube del Gobierno de España.
  - Autofirma.
  - Port@firmas.
  - Firma por evidencias de firma de Cl@ve2 (ver página 24).
  - Adobe Acrobat Reader: Este método no debe usarse, pues es propietario y normalmente incompatible con los procesos de firma del tramitado y portafirmas.
  - Pendientes de integración con FIRe ( https://administracionelectronica.gob.es/ctt/fire) con certificados alojados en la nuebes del Gobiernos de España.

# Dispositivos seguros de firma electrónica.

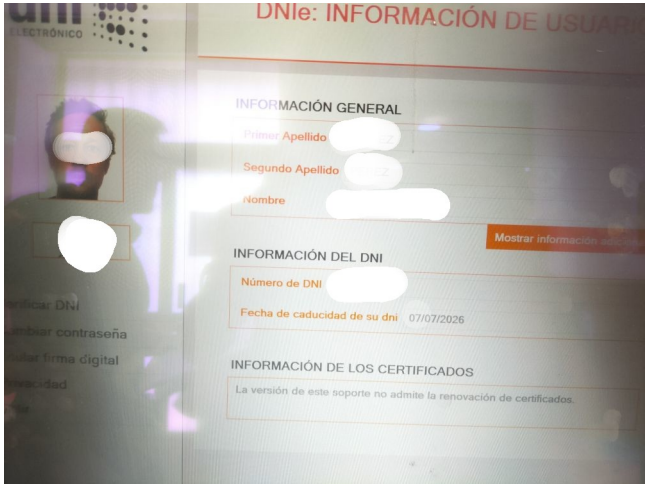
- El DNIe contiene un chip critográfico para almacenamiento «seguro» de certificados (del DNI).
- Para el uso del DNIe es preciso:
  - Disponer de un lector de tarjetas criptográfica.
  - Tener instalados los componentes del DNIe (ver página 23).
- Según

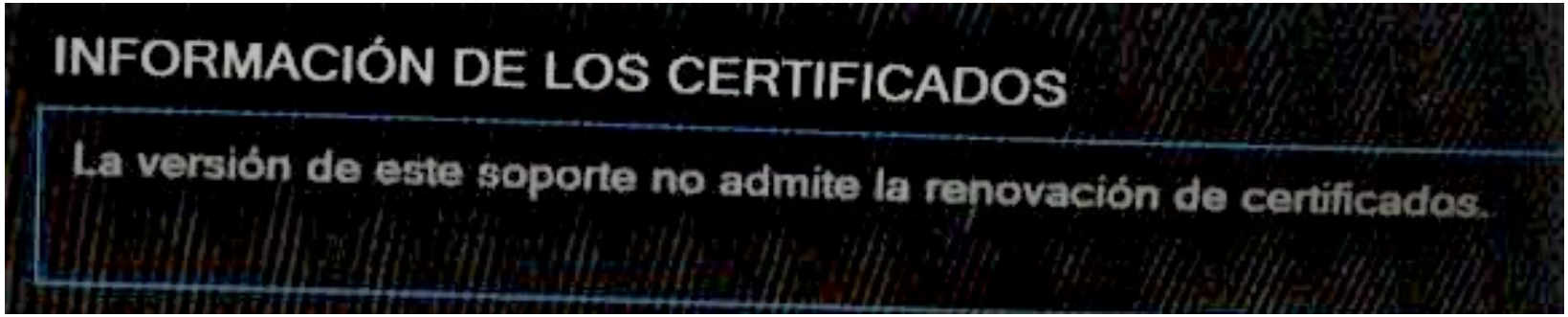
  https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1004&id_menu=42

  sus certificados tienen una vigencia máxima de 5 años. A mí no me ha durado más de 2.

# Dispositivos seguros de firma electrónica.

- Soporte DNIe
  vulnerable y/o con problemas:



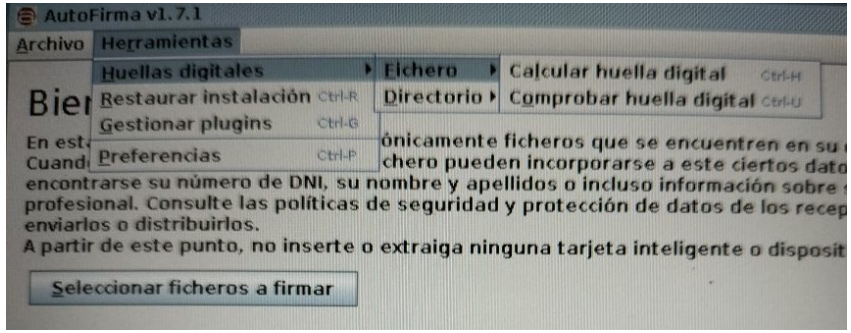



# Dispositivos de validación.

- @Firma, modelo federado y modelo nube del Gobierno de España.
- Port@firmas.
- Aplicación corporativa https://ov.dipalme.org/csv
- Aplicación del ministerio https://valide.redsara.es
- DNIe: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_320&id_menu=15

# Generación y validación de huellas

- Autofirma posee una utilidad para la generación y comprobación de huellas criptográficas (ver página 12).
- Mediante «Calcular huella digital» se calcula la huella de un fichero dado. Aconsejo base-64 y SHA-512.
- Mediante «Comprobar huella digital» se comprueba que la huella corresponda al fichero.




- Para firmar **fichero grandes**, por impedimento de Port@firma y la oficina virtual, se debe generar un documento de firma que haga referencia al documento de partida original, y se le indica (copiada textualmente) la huella en base-64. Este es el documento que debe firmarse.

# Certificado electrónico.

- El propósito de los certificados es el de proveer una clave o llave binaria que permita encriptar y/o desencriptar datos mediante la única utilización de estas y los algoritmos pertinentes.
- Existen dos tipos principales: claves simétricas (1 sola que encripta y desencripta), claves asimétricas (2 de modo que lo que una encripta sólo la otra lo puede desencriptar y viceversa).
- En el contexto de la firma electrónica cualificada, un certificado:
  - Son dos conjuntos de datos íntimamente relacionados, conocidos como clave pública y clave privada (claves asimétricas).
  - Lo que se encripta con la clave privada solo puede ser desencriptado con la clave pública.

# Certificado electrónico.

- Ambas claves han sido generadas por una autoridad de certificación (CA) cualificada conforme a la legislación española (ver página 42).
- La clave pública está firma por la autoridad certificadora para dar fe de que es la generada por dicha autoridad.
- Ambas claves están contenidas normalmente en un único fichero con formato PKCS12 (ficheros «`*.p12`», «`*.pfx`»), conocido como certificado.

# Certificado electrónico.

- La clave pública tiene el formato X.509 y posee asociada un conjunto de datos de la persona o institución para la cual se expide.
- Al estar firmada por la autoridad de certificación constituye por sí misma un mecanismo de identificación, pues la autoridad debe haberse asegurado de que los datos son correctos y pertenecen a quien va destinado el certificado.
- **La clave privada no puede bajo ningún concepto hacerse pública a nadie ni cederse**, mientras que la clave pública se puede o debe compartir en los procesos de firma (¡Cuidado! Contiene los datos personales).

# Certificado electrónico.

- Los certificados tienen un **periodo de validez** (normalmente 2 o 3 años).
- Un certificado al cual le ha superado el periodo de validez se le llama **expirado**.
- Un certificado puede ser invalidado por la autoridad de certificación (porque se haya comprometido su seguridad, por ejemplo). Estos certificados se denominan **revocados**.

# Certificado electrónico.

- Los certificados electrónicos pueden ser (algunos principales):
  - DNIe: expedido por la Policía Nacional.
  - Personales o de persona física: normalmente expedido por FirmaProfersional.
  - De funcionario: normalmente expedido por FirmaProfersional.
  - De representación.
  - De sello de entidad: normalmente expedido por FirmaProfersional.
  - De sede: normalmente expedido por FirmaProfersional.
  - De sitio: actualmente expedidos por Let’s Encrypt, FirmaProfersional, otros.

# Certificado electrónico.

- Para comprobar la validez de un certificado es preciso:
  - Comprobar que no está expirado (mediante comprobación de su fecha fin de validez).
  - Que no está revocado.
  - Que ha sido emitido por una autoridad de certificación cualificada.
  - Que está correctamente firmado por la autoridad de certificación.
- Estas comprobaciones se realizan mediante llamadas a servicios OCSP de la autoridad de certificación o mediante la consulta de listas de certificados revocados (CRL) que publican.

# Informe de firmas.

- Muy habitualmente se confunde el informe de firmas con la firma: ¡ERROR!
- El informe de firmas no está firmado y es manipulable. Se puede alterar su contenido.
- El informe de firmas sólo vale para obtener datos visuales de la firma (no fidedignos) y acceso por CSV al documento de partida original, su informe y su firma.

| Código Seguro De Verificación | lQrsTrR8FSTLntPQFR5p7Q== | Estado | Fecha y hora |
|---|---|---|---|
| Firmado Por | Andrés Orencio Ramírez Pérez - Jefe de Sección de Bases de Datos y Coordinación de Aplicaciones | Firmado | 14/09/2022 10:38:35 |
| Observaciones | | Página | 1/1 |
| Url De Verificación | https://ov.dipalme.org/verifirma/code/lQrsTrR8FSTLntPQFR5p7Q%3D%3D | | |
| Normativa | Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015). | | |

# Ejercicios.

- Ejercicio:
  - Comprobar datos de certificado.
  - Validar certificado.
  - Validad DNIe.
  - Firmar documento (CaDES, PaDES).
  - Validar documento firmado.
  - Manipulación de informe de firmas.

# Enlaces.

- Lista de autoridades de certificación de confianza y cualificados, y prestadores de servicios electrónicos de confianza cualificados:

  https://sedeaplicaciones.minetur.gob.es/Prestadores/
- Obtención de certificados de la FNMT:

  https://www.cert.fnmt.es/certificados
- Autofirma: https://firmaelectronica.gob.es/Home/Descargas.html
- DNIe: Área de descargas https://www.dnielectronico.es/PortalDNIe/
- Firefox: https://www.mozilla.org/es-ES/firefox/new/

# Documento y expediente electrónico.

- Tanto un documento como un expediente electrónico es aquel que tiene asociados un conjunto de metadatos conforme a la especificación ENI.
- Información:
  https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html
- Comprobación de documentos y expedientes electrónicos:

  https://sede.administracion.gob.es/pagSedeFront/servicios/validarENI.htm
- Se exportan y transfieren como ficheros XML.
- Ver página 8.