Firma electrónica

Diputación Provincial de Huesca

Huesca, octubre de 2017

José Félix Muñoz Soro
Laboratorio Jurídico-Empresarial de la Universidad de Zaragoza
Parque Tecnológico Walqa

CONTENIDO

© J. F. Muñoz Soro - 2017

IDENTIFICACIÓN Y AUTENTIFICACIÓN
identificación

La identificación se refiere a las personas

su objetivo es saber quien está accediendo a una operatoria

Los medios que se utilizan pueden ser
- algo que se sabe
  - contraseñas y PIN
- algo que se tiene
  - tarjetas y claves criptográficas
- algo que se es
  - medidas biométricas

Autenticación con certificados

«factor de autenticación basado en la posesión»: factor de autenticación en el que el sujeto está obligado a demostrar la posesión;

«factor de autenticación basado en el conocimiento»: factor de autenticación en el que el sujeto está obligado a demostrar conocimiento del mismo;

«factor de autenticación inherente»: factor de autenticación que se basa en un atributo físico de una persona física del cual el sujeto está obligado a demostrar su posesión;

IDENTIFICACIÓN Y AUTENTIFICACIÓN
clases de medios de identificación

Según la función
- personal
  - regulada por el Estado
  - medios robustos de identificación
- corporativa
  - vinculo con una organización
- de cliente
  - relación de negocio

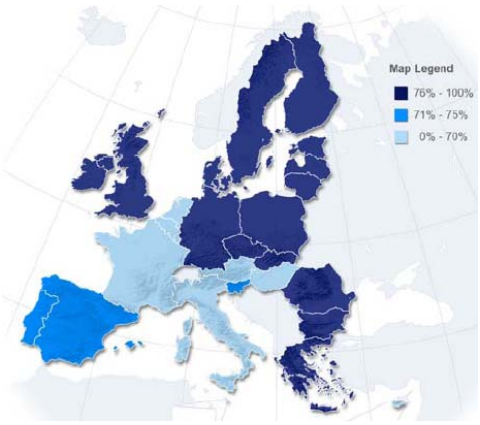
Según el emisor
- de tercera parte
  - relación con entidades ajenas al emisor
- de segunda parte
  - relaciones con el emisor
- de primera parte
  - lo emitimos nosotros mismos

IDENTIFICACIÓN Y AUTENTIFICACIÓN
el identificador único

Se considera un riesgo para la privacidad
- Constitución de Portugal
  - art. 35, 5º. Se prohíbe la atribución a los ciudadanos de un número nacional único

En España, el DNI se introduce en 1951
- y tiene un amplia aceptación

En el otro extremo: los países anglosajones
- hay una fuerte resistencia a su implantación

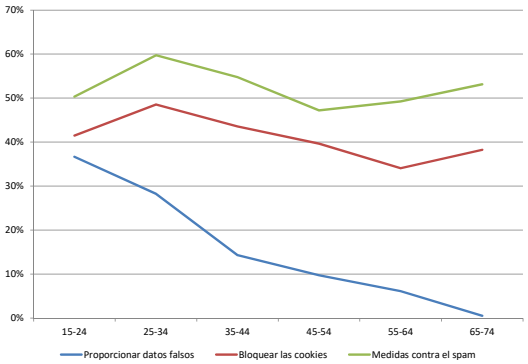


Eurobarometro 2011 - Consider their national identity number, identity card number or passport number as personal information

IDENTIFICACIÓN Y AUTENTIFICACIÓN
la identidad en las redes

Utilizamos múltiples identidades
- para múltiples fines
- nos permiten proteger mejor nuestra información personal

Incluso falsas
- por seguridad informática
- anonimato
  - por razones políticas y profesionales



OASI 2006-2009 - Medidas de autoprotección (por edad)

IDENTIFICACIÓN Y AUTENTIFICACIÓN
requisitos que deben cumplir los documentos electrónicos

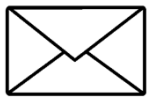
autenticidad de origen

integridad

= firma electrónica =

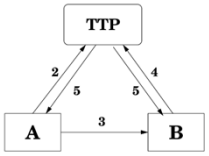
confidencialidad

= cifrado de confidencialidad =



no repudiación

= terceros confiables (TTP) =



IDENTIFICACIÓN Y AUTENTIFICACIÓN
autenticación o autentificación

Se refiere a los documentos

documento autentico

Los medios utilizados deben garantizar
- la autenticidad del origen
- la garantía de integridad

Se utiliza la firma electrónica

Autenticación o autentificación son sinónimos
- pero en los ámbitos técnicos se suele denominar autenticación a la identificación
  - también lo hace el Reglamento eIDAS

IDENTIFICACIÓN Y AUTENTIFICACIÓN
normativa sobre firma electrónica

Reglamento UE 910/2014 del P. E. 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 el que se deroga la Directiva 1999/93/CE

- conocido como Reglamento eIDAS
- aplicable desde el 1 de julio de 2016
- deroga la Directiva 1999/93, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica

La Ley 59/2003, de 19 de diciembre, de firma electrónica, subiste en lo que no se oponga directamente al Reglamento

IDENTIFICACIÓN Y AUTENTIFICACIÓN
firma electrónica no avanzada

Son los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar

Reglamento eIDAS, articulo 3, 10

La más utilizada son las contraseñas

- resultan fáciles de implementar y de usar
- su debilidad radica en que son conocidas por aquel que proporciona los medios de firma
  - y en el robo de contraseñas

IDENTIFICACIÓN Y AUTENTIFICACIÓN
firma electrónica avanzada

Una firma electrónica avanzada cumplirá los requisitos siguientes:

- estar vinculada al firmante de manera única
- permitir la identificación del firmante
- haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
- estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Reglamento eIDAS, articulo 26

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
la criptografía

Criptografía
- es el arte de escribir oculto
- origen en la Grecia clásica
  - scitala, Esparta, 400 a.C.

Criptoanálisis
- busca la forma de romper los cifrados

Esteganografía
- ocultar un mensaje

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
criptografía clásica o de clave simétrica

se emplea la misma clave para cifrar y descifrar

algoritmos
- DES (Data Encryption Standard), 1974
- AES (Advanced Encrytion Standard), 2002

es más eficiente
- se sigue utilizando para el cifrado de confidencialidad

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
la criptografía moderna o de claves asimétricas

hay dos claves relacionadas
- lo que se cifra con una se descifra con la otra
- conociendo una no es posible deducir la otra
- las llamamos clave pública y clave privada

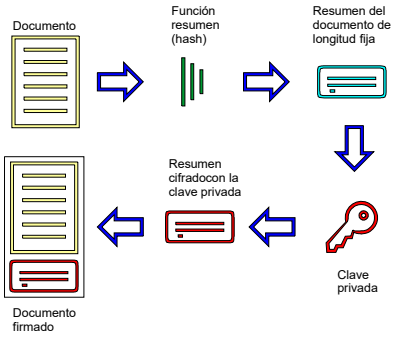
origen
- Whitfield Diffie & Martin Hellman (1976)

algoritmos
- RSA (Rivest, Shamir y Adleman)

PGP (*Pretty Good Privacy*)
- Phil Zimmermann , 1991

PKI
Public Key Infrastructure

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
generación de la firma

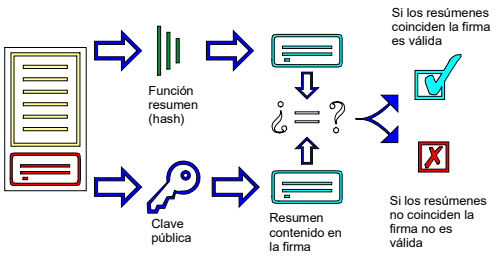


Se genera un resumen del documento (función *hash)*

El resumen cifrado con la clave privada del firmante constituye la firma electrónica de este

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
comprobación de la firma

Por una parte se calcula el resumen del documento



Por otra, se descifra la firma utilizando la clave pública del firmante

Si ambos resúmenes coinciden la firma es correcta y sabemos

que la firma corresponde al firmante y al documento (autenticidad)

que el documento no ha sido modificado (integridad)

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
el cifrado de confidencialidad

El cifrado de confidencialidad permite ocultar el contenido de documentos y comunicaciones

Cualquiera puede enviarnos un documento cifrado

- utilizando la clave pública que contiene nuestro certificado
- sólo el destinatario usando su clave privada podrá descifrar el contenido del mensaje

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
los certificados electrónicos

La clave pública es el mecanismo de comprobación de las firmas electrónicas, pero ¿cómo podemos saber que una clave pública pertenece a una persona dada?

Para ello se crean Servicios de Certificación o CA

- las CA (Certification Authority) emiten certificados electrónicos que asocian una identidad con una clave pública
- los certificados están firmados por la CA, por lo que ésta debe difundir sus claves

En el trámite de registro se comprueba la identidad del signatario y se recoge su compromiso con las claves certificadas

- Autoridades de Registro o RA (Registry Authority)

CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
el tiempo

La autenticación de un documento incluye la referencia al momento en el que fue creado

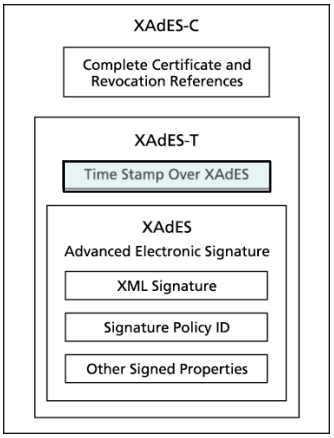
sello de tiempo (*time stamp*)

un prestador de servicios de confianza certifica con su firma la fecha y hora

marca de tiempo

es una referencia temporal no respaldada por la firma de un prestador de servicios de confianza

Las firmas que se utilizan en la tramitación están formadas por la firma más el sello de tiempo



CÓMO FUNCIONA LA FIRMA ELECTRONICA AVANZADA
estándares más importantes

Formato de los certificados
- X-509, Unión Internacional de Telecomunicaciones

PKI
- normas ETSI de la Unión Europea

Publicación de los certificados revocados
- CRL
  - Certificate Revocation List
    - se está dejando de usar
- OCSP
  - On line Certificate Status Protocol

ETSI
319 401 v2.1.1 General Policy Requirements for Trust Service Providers
319 411 Policy and security requirements for Trust Service Providers issuing certificates
- 319 411-1 v1.1.1: General requirements
- 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates

319 412 Certificate Profiles
- 319 412-1 v1.1.1: Overview and common data structures
- 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons
- 319 412-5 v2.1.1: QCStatements

319 421 v1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles
102 573 v2.1.1 Policy requirements for trust service providers signing and/or storing data objects.
102 853 v1.1.2 Signature validation procedures and policies

LOS CERTIFICADOS ELECTRONICOS
tipos de certificados

firma electrónica
personas físicas

sello electrónico
personas jurídicas

certificados personales
personas físicas que actúan en su propio nombre

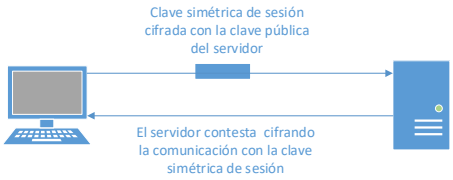
certificados de cargo o representación
personas físicas que actúan en nombre de una persona jurídica

Por ejemplo: facturas o actuación automatizada

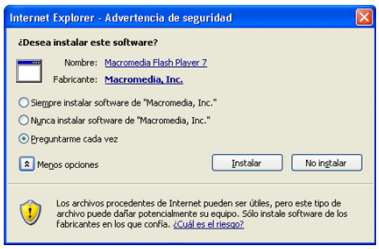
LOS CERTIFICADOS ELECTRONICOS
los certificados de “componentes”

Certificados de servidor
- identifican a un servidor informático
  - y permiten cifrar la comunicación con el mismo
- su presencia se indica en el navegador con un candado cerrado y por el https: en la barra de direcciones
  - *Reglamento eIDAS, articulo 45*

Firma de software
- permiten firmar las aplicaciones y apps



SSL
(*Secure Socket Layer*)



LOS CERTIFICADOS ELECTRONICOS
la firma electrónica cualificada

Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita

no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada

Reglamento eIDAS, articulo 25

Firma electrónica cualificada

una firma electrónica avanzada que se crea

mediante un dispositivo cualificado de creación de firmas electrónicas

y que se basa en un certificado cualificado de firma electrónica

Reglamento eIDAS, articulo 3, 12

LOS CERTIFICADOS ELECTRONICOS
contenido de los certificados cualificados

- Indicación de que es un certificado cualificado
- Conjunto de datos que represente inequívocamente al PSC
- nombre del firmante o un seudónimo

  si se usa un seudónimo, se indicará claramente
- Datos de validación de la firma electrónica
- Inicio y final del período de validez del certificado;
- Código de identidad del certificado
- Firma electrónica avanzada o el sello electrónico del PSC

  debe indicarse el lugar en que está disponible gratuitamente
- La localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado
- Cuando los datos de creación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto

Reglamento eIDAS, anexo I

LOS CERTIFICADOS ELECTRONICOS
la firma en la nube

El requerimiento de que la clave privada esté bajo el exclusivo control del firmante plantea es incompatible con las aplicaciones en la nube

La Ley de firma electrónica decía
que ha sido creada por medios que el firmante puede mantener **bajo su exclusivo control**
fue modificada en 2015

Firma electrónica avanzada
haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, **con un alto nivel de confianza**, bajo su control exclusivo
Reglamento eIDAS, articulo 26

Se permite la gestión de firmas por parte de los PSC

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
concepto

Es una persona física o jurídica que presta uno o más servicios de confianza (*Reglamento eIDAS, articulo 3, 19)*

Principio del mercado interior (*Reglamento eIDAS, articulo 4)*

El Reglamento eIDAS establece un marco más amplio

de los servicios de certificación se pasa a los servicios de confianza

Los servicios de confianza que contempla el Reglamento eIDAS son:
- certificación de firma y sellos electrónicos
- validación de firmas y sellos electrónicos
- sellado de tiempo (*time stamping*)
- entrega certificada
- conservación de firmas

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
los prestadores cualificados

Verificará la identidad y cualquier atributo específico
en presencia de la persona física o por
medios con una seguridad equivalente

Requisitos
- obligaciones de información
- personal especializado
- recursos financieros suficientes o seguros
- utilizarán sistemas y productos fiables
- tomarán medidas adecuadas contra la falsificación y el robo de datos
- registrarán y mantendrán accesible durante un período de tiempo la información
- contarán con un plan de cese actualizado
- tratamiento lícito de los datos personales
- mantener una base de datos de certificados

etiqueta de confianza «UE» para servicios de confianza cualificados

REGLAMENTO DE EJECUCIÓN (UE) 2015/806 DE LA COMISIÓN de 22 de mayo de 2015

Reglamento eIDAS, articulo 24

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
listas de confianza

Cada Estado miembro establecerá, mantendrá y publicará listas de confianza con los prestadores cualificados de servicios de confianza
y los servicios que prestan

Se publican en forma apta para su tratamiento automático

Cada Estado debe notificar a la UE información sobre el organismo responsable de las listas de confianza nacionales, y detalles relativos al lugar en que se publican dichas listas.

DECISIÓN DE EJECUCIÓN (UE) 2015/1505 DE LA COMISIÓN de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento eIDAS

Reglamento eIDAS, articulo 22

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
sistema de notificación

Los Estados miembros deberán reconocer los medios de identificación electrónica pertenecientes a un sistema de identificación electrónica notificado por otro Estado miembro

reconocimiento mutuo

Reglamento eIDAS, artículos 1 y 6

Condiciones para la notificación

que el Estado de origen los acepte en al menos un servicio
que cumpla con uno de los niveles de seguridad
que el estado del certificado su publique en línea
que cumple con los requerimientos de interoperabilidad

Reglamento eIDAS, articulo 7

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
niveles de seguridad

Se definen tres niveles de seguridad
- bajo
- sustancial
- alto

Reglamento eIDAS, articulo 8

Se tienen en cuenta aspectos como:
- inscripción
  - solicitud y registro
  - prueba y verificación de la identidad
  - vinculación entre personas físicas y jurídicas
- gestión de los medios de identificación
- gestión de la seguridad
- instalaciones y personal
- controles técnicos
- cumplimiento y auditoria

REGLAMENTO DE EJECUCIÓN (UE) 2015/1502 DE LA COMISIÓN de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento eIDAS

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
cooperación e interoperabilidad

Se establece un marco de interoperabilidad

Los Estados deben cooperar respecto a

- la interoperabilidad de los sistemas
- la seguridad de los sistemas

La cooperación consiste en

- intercambio de información y experiencias
- revisión *inter pares* de los sistemas
- examen de las novedades

Reglamento eIDAS, articulo 12

DECISIÓN DE EJECUCIÓN (UE) 2015/296 DE LA COMISIÓN de 24 de febrero de 2015 por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al artículo 12, apartado 7, del Reglamento eIDAS

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
prestadores más importantes en España

Sector privado
- Verisign, Globalsign, IPSCA, ANF, …

Fedatarios y registradores
- Ancert y SCR

Sector publico
- FNMT
- CatCert
- Izempe

Cámaras de Comercio
- Camerfirma

DNI electrónico

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
la FNMT

Es el servicio de certificación para la AGE
- Ley de acompañamiento a los presupuestos para 1998; desarrollado por RD 1317/2001

Lo es también de la DGA
- convenio de 21 de noviembre de 2005
- y de las entidades locales que se acojan

Autoridad de certificación para la Administración publica española (AC APE)
- clases de certificados
  - de personal al servicio de las AP
  - identificación de sede electrónica
  - actuación administrativa automatizada (sello)
- también es autoridad de sellado de tiempo

LOS PRESTADORES DE SERVICIOS DE CONFIANZA
DNI electrónico

El DNI electrónico es el medio personal de identificación por excelencia
- regulado por el Estado
- se basa en documentos robustos de identificación física
- es una identidad “base” que permite obtener otros medios de identificación

Nos identifica como ciudadanos
- sin conexión con ninguna organización

Declaración de prácticas, Orden INT/738/2006
- certificado de autenticación: identificación
- certificado de firma: firmar trámites y documentos

Es certificado reconocido
- puede sustituir a la firma manual
- no se establecen limitaciones

LAS POLITICAS Y LA DECLARACION DE PRACTICAS
concepto

Las Políticas establecen los compromisos del prestador de servicios de confianza
- en la Declaración de prácticas el prestador detalla la forma en la que lleva a cabo lo establecido en las Políticas y cumple con los compromisos asumidos en las mismas

Los prestadores de servicios de confianza deben disponer obligatoriamente de una Declaración de prácticas (*Ley de firma electrónica, articulo 19*)
- por lo general disponen también de Políticas para las distintas clases de certificados
  - son los documentos que nos permiten saber para que se puede utilizar un certificado
    - y, por tanto, el valor jurídico de la firma electrónica respaldada por ese certificado

LAS POLITICAS Y LA DECLARACION DE PRACTICAS
aspectos generales

Descripción general
- quien el PSC, personalidad jurídica, domicilio, etc.

Participantes
- el propio PSC
- las autoridades de registro
- los suscriptores
- los terceros aceptantes

Usos permitidos y prohibidos de los servicios

Publicación
- de la Declaración y de las Políticas
- de los certificados utilizados en la prestación de los servicios

LAS POLITICAS Y LA DECLARACION DE PRACTICAS
operatoria

Denominación de los suscriptores
- formación del nombre
- seudónimos

Validación de la identidad del suscriptor y obtención del consentimiento

Proceso de la solicitud y emisión del certificado

Renovación

Suspensión y revocación

Publicación de los certificados y su estado
- directorio OCSP (*Online Certificate Status Protocol*)

LAS POLITICAS Y LA DECLARACION DE PRACTICAS
medidas de seguridad

Medidas de seguridad de nivel físico
Controles de procedimiento
Controles de personal
Procedimientos de registro de auditoría
Documentos archivados
Compromiso y recuperación de desastres
Terminación de la actividad del PSC
Controles de seguridad técnica
Generación e instalación de pares de claves
Protección de las claves privadas y módulos criptográficos
Datos de activación
Controles de seguridad de las computadoras
Controles técnicos del ciclo de vida
Controles de seguridad en las redes

LAS POLITICAS Y LA DECLARACION DE PRACTICAS
auditorias

Los PSC deben someterse obligatoriamente a auditorías periódicas

En la Declaración de prácticas debe especificarse
- la frecuencia de las auditorias
  - debe ser como mínimo anual
- identidad y cualificación del evaluador
- relación del evaluador con la entidad evaluada
  - al menos cada dos años el auditor debe ser externo
  - se debe garantizar la independencia
    - tanto si es interno como externo
- temas tratados por la auditoria
- medidas adoptadas como consecuencia de una deficiencia
- comunicación de los resultados de la auditoria

NORMATIVA ADMINISTRATIVA SOBRE IDENTIFICACIÓN Y FIRMA
aspectos jurídicos y otras cuestiones

Precios

Responsabilidad financiera
- debe disponerse de una garantía de al menos 3 millones de euros

Confidencialidad de la información comercial, privacidad de la información personal y derechos de propiedad intelectual

Compromisos y garantías, limitación de las garantías, limitaciones de la responsabilidad, indemnizaciones

Vigencia de la Declaración de prácticas y modificaciones

Legislación aplicable y disposiciones relativas a la solución de controversias

NORMATIVA ADMINISTRATIVA SOBRE IDENTIFICACIÓN Y FIRMA

la nueva regulación de la LRJSP y la LPAC

La administración electrónica deja de considerarse como un canal superpuesto al normal, basado en el soporte papel

y pasa a ser el medio estándar para el funcionamiento de las Administraciones

Las leyes 39/2015 (LPAC) y 40/2015 (LRJSP)

integran la regulación contenida en la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos

sin introducir grandes cambios

Sistematizan la normativa sobre la materia

Objetivo
la Administración sin papel

Medio
los documentos electrónicos

NORMATIVA ADMINISTRATIVA SOBRE IDENTIFICACIÓN Y FIRMA

derechos de la ciudadanía en la LPAC

Derechos de las personas *(LPAC, título II, capitulo I, artículos 13 y 14)*
- a acceder al Punto de Acceso General electrónico de la Administración
- a ser asistido en el uso de medios electrónicos
- a la obtención y utilización de los medios de identificación y firma electrónica
- a elegir en todo momento el medio por el que se comunican con las AAPP
  - hay numerosas excepciones

Derechos del interesado *(LPAC título IV, capitulo I, artículo 53)*
- a identificar al personal responsable del procedimiento
- a no presentar documentos originales
- a obtener copias electrónicas autenticas de los documentos administrativos

NORMATIVA ADMINISTRATIVA SOBRE IDENTIFICACIÓN Y FIRMA

regulación en la LRJSP y en la LPAC

La LRJSP establece los medios de identificación y firma de las AA. PP. y sus empleados *(LRJSP título preliminar, capitulo V)*

- sede electrónica y portal de internet
- identificación de las AAPP
- actuación administrativa automatizada
- firma electrónica del personal de la AAPP
- entornos cerrados de comunicación
- archivo

La LPAC regula el uso de medios de identificación y firma por los interesados *(LPAC título I)*

- sistemas de identificación de los interesados
- sistemas de firma admitidos por las AA. PP.
- obligatoriedad del uso de firma
- asistencia en el uso de la firma
- registros electrónicos de apoderamientos

NORMATIVA ADMINISTRATIVA SOBRE IDENTIFICACIÓN Y FIRMA

la distinción entre identificación y firma

Aunque se trata de una diferencia clara desde el punto de vista técnico, la legislación no la recogía de forma apropiada

ahora se distinguen en todo momento ambas operaciones

La identificación será suficiente para cualquier actuación, salvo en los siguientes supuestos para los que se requerirá la firma *(LPAC artículo 11)*

- formular solicitudes
- presentar declaraciones responsables o comunicaciones
- interponer recursos
- desistir de acciones y renunciar a derechos

Se pretende facilitar la realización de trámites, pero lo importante es que medios se exigen para la identificación y para la firma.

IDENTIFICACIÓN Y FIRMA DE LAS AA. PP.
identificación de las Administraciones

Las Administraciones públicas se identifican mediante un sello electrónico *(LRJAP art. 40)*

- basado en un certificado electrónico cualificado
- el certificado debe contener
  - el número de identificación fiscal
  - la denominación
  - la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos

La lista de los sellos debe publicarse en la sede electrónica

Las sedes electrónicas se identifican mediante certificados de servidor *(LRJAP art. 38)*

IDENTIFICACIÓN Y FIRMA DE LAS AA. PP.
firma para la actuación administrativa automatizada

Actuación automatizada es la realizada íntegramente a través de medios electrónicos (LRJSP art. 41)

- sin intervención directa de un empleado público
- son actos cuyo contenido viene determinado de forma univoca por una norma o meras comunicaciones de información
  - como un acuse de recibo o una certificación de vida laboral

Pueden firmarse con (LRJSP art. 42)
- un sello electrónico
- un código seguro de verificación

IDENTIFICACIÓN Y FIRMA DE LAS AA. PP.
el código seguro de verificación

En lugar de los documentos auténticos utilizamos **imágenes electrónicas** (o en soporte papel) de los mismos

con un código que permite acceder al documento autentico obrante en el archivo del organismo

y comprobar la fidelidad de la imagen

Cód. Validación: 9AYG9DNNS3X2Z3CHRXSL2PEQL | Verificación: http://alagon.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 1 de 1

IDENTIFICACIÓN Y FIRMA DE LAS AA. PP.
firma de los empleados públicos

Los actos de las Administraciones se autentican mediante la firma electrónica del titular del órgano o empleado público (LRJAP artículo 43)

Cada Administración decide los sistemas de firma electrónica que utiliza su personal

certificados de empleado

son certificados de persona física

identifican también la organización

y pueden contener el puesto o cargo

puede utilizarse el DNI electrónico

Por motivos de seguridad se puede incluir únicamente el número de identificación profesional del empleado público

ancert Agencia Notarial de Certificación

Certificados para Corporaciones de Derecho Público

Personal al servicio de las Administraciones públicas

SCR Servicio de Certificación de los Registradores

Certificado de Cargo Administrativo

¿Y los responsables políticos?

IDENTIFICACIÓN Y FIRMA DE LAS AA. PP.
entornos cerrados de comunicación

Los entornos cerrados de comunicaciones son las intranets establecidas entre las Administraciones.

Los documentos recibidos a través de las mismas se consideran auténticos, según las siguientes reglas (LRJAP art. 44)

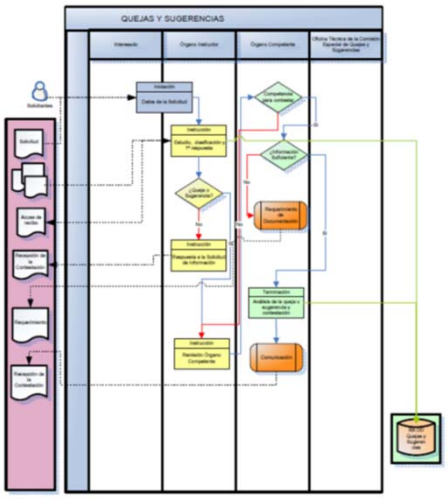
- si la intranet es de una Administración ésta determina las condiciones y garantías
  - que, al menos, incluirán la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar
- si une a distintas Administraciones las condiciones se establecen mediante convenio

IDENTIFICACIÓN Y FIRMA DE LAS AA. PP.
requerimientos e interoperabilidad

Cada Administración determina que trámites deben incluir firma electrónica avanzada (LRJAP art. 45)

Cuando una Administración utiliza a nivel interno sistemas de firma no interoperables

- puede superponer a los documentos firmados un sello electrónico interoperable
  - que puede ser reconocido por otras Administraciones



IDENTIFICACIÓN Y FIRMA DE LOS INTERESADOS
identificación de los interesados

Las Administraciones Públicas están obligadas a **verificar** la identidad de los interesados en el procedimiento administrativo (LPAC artículo 9)

Los interesados pueden identificarse electrónicamente mediante cualquier sistema que se base en un registro previo

- certificados electrónicos reconocidos o cualificados de firma electrónica
  - lista de confianza de prestadores de servicios de certificación
- claves concertadas y cualquier otro sistema que las Administraciones consideren válido
  - en los términos y condiciones que establezcan

Ley 11/2007 art. 13, c)

Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

IDENTIFICACIÓN Y FIRMA DE LOS INTERESADOS
firma de los interesados

Los interesados pueden firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento (LPAC art. 10)

Se consideran válidos a efectos de firma:

- sistemas de firma electrónica y sellos basados en certificados electrónicos reconocidos o cualificados
  - lista de confianza de prestadores de servicios de certificación
- cualquier otro sistema que las Administraciones consideren válido, en los términos y condiciones que se establezcan.

Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá acreditada mediante el propio acto de la firma

IDENTIFICACIÓN Y FIRMA DE LOS INTERESADOS
política de firmas

Cada Administración Pública podrá determinar que sistemas admite (LPAC art. 9 y 10)

la admisión de un sistema de identificación no avanzado obliga a admitir los avanzados

La aceptación de un sistema por la AGE servirá para acreditar frente a todas las Administraciones la identificación electrónica de los interesados

Las Administraciones podrán admitir los sistemas de identificación como sistema de firma

si permiten acreditar la autenticidad de la expresión de la voluntad y el consentimiento

DECISIÓN DE EJECUCIÓN (UE) 2015/1506 DE LA COMISIÓN de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento eIDAS

IDENTIFICACIÓN Y FIRMA DE LOS INTERESADOS
asistencia a los interesados

Las Administraciones deben garantizar que los interesados pueden relacionarse con ellas a través de medios electrónicos (LPAC art.12)

disponiendo de los canales, los sistemas y aplicaciones precisos

Deben asistir en el uso de medios electrónicos a las personas físicas no profesionales

su identificación o firma podrá ser realizada por un funcionario público

el interesado debe prestar su consentimiento expreso

del que deberá quedar constancia

deben publicar un registro con los funcionarios habilitados para esta función

IDENTIFICACIÓN Y FIRMA DE LOS INTERESADOS
los apoderamientos

La LPAC prevé la creación de Registros electrónicos de apoderamientos *(LPAC artículo 61)*

- cada Administración debe disponer de un registro electrónico general de apoderamientos
- puede haber registros particulares en cada organismo

No se contempla la utilización de certificados de cargo o representación

SCR Servicio de Certificación de los Registradores

firmaprofesional

certificados de atributos

IDENTIFICACIÓN Y FIRMA DE LOS INTERESADOS
las notificaciones electrónicas

Dos medios *(LPAC artículo 43)*

- comparecencia en la sede electrónica dirección electrónica habilitada única

Se exige el acceso por el interesado o su representante debidamente identificado

Se entenderá rechazada cuando hayan transcurrido diez días naturales

- desde la puesta a disposición en la sede electrónica o en la dirección electrónica habilitada única

Dirección Electrónica Habilitada

Servicio de entrega electrónica certificada
Reglamento eIDAS articulo 43

CONSERVACION DE LAS FIRMAS ELECTRONICAS
la caducidad de las firmas electrónicas

Las firmas electrónicas pierden su valor al cabo del tiempo por distintas razones

- al caducar el certificado que la respalda ya no es posible verificar la firma electrónica
  - la firma electrónica se basa en la combinación de dos elementos: los datos de creación de firma y los datos de comprobación de firma (el certificado)
- razones tecnológicas
  - por dejar de considerarse segura la longitud de clave utilizada
  - obsolescencia de los algoritmos

CONSERVACION DE LAS FIRMAS ELECTRONICAS
mecanismos para la conservación de las firmas

Firmas longevas

- se añade la información del estado del certificado, un sello de tiempo y los certificados que forman la cadena de confianza

Otros métodos técnicos que impidan la modificación de la firma para la que se ha verificado su validez

- todos los cambios que se realicen podrán auditarse para asegurar que dicha firma no ha sido modificada
- cumplir los requisitos de seguridad del Esquema Nacional de Seguridad

Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración

Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas

Gracias por su atención

jfm@unizar.es