

La firma en la Administración Electrónica

Manuel Vázquez
vazquez@unizar.es

Grupo LEFIS – Departamento de Matemáticas – Universidad de Zaragoza



2^{as} Jornadas
sobre Derecho
y Tecnología

9^o Encuentro
Ibero-Latinoamericano
de Gobierno Electrónico
e Inclusión Digital

28-29 de junio 2010
Universidad de Valladolid

UVa



LEFIS
LEGAL FRAMEWORK FOR THE INFORMATION SOCIETY

Ley 59/2003, de Firma Electrónica

establece (progresivamente) los requisitos para que una firma electrónica goce de plena confianza

Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos (2007)

regula las relaciones electrónicas entre la Administración y los ciudadanos

Ley de Firma Electrónica

La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel

Real orden de 12 de febrero de 1900, Gaceta de Madrid de 19 de febrero

SM el REY (QDG), y en su nombre la REINA Regente del Reino, ha tenido á bien disponer que en todas las oficinas del Estado, provinciales y municipales se admitan cuantas instancias y documentos se presenten hechos con máquinas de escribir, en los mismos términos y con iguales efectos de los escritos ó copiados á mano.

características

- no existe ninguna regulación jurídica
- goza de de confianza
- fácilmente imitable
- salvo en casos sensibles, no se comprueba su autenticidad
- en caso de prueba es necesario el concurso de terceras personas (testigos, notario, grafólogos, etc)
- existe un documento original
- existe abundante bibliografía que propugna la firma manuscrita como un procedimiento biométrico para el acceso a las tecnologías de la información (tesis doctoral de Juan Manuel Pascual, UVA, 2009)

USOS

- como forma de autenticación
- como prueba de aceptación y conformidad con el documento firmado

- *Firma electrónica (simple)*: conforme a las condiciones acordadas por las partes para relacionarse entre sí. El remite de un email, el pin de una tarjeta de crédito
- *Firma electrónica avanzada*, la que se basa en un sistema de clave pública: PGP, la utilizada en MSWord
- *Firma electrónica avanzada y certificada*, es la que está garantizada por un prestador de servicios, cumpliendo algunas de las obligaciones anteriores: Lefis, CertiVer
- *Firma electrónica basada en certificado no reconocido*, garantizada por un prestador de servicios de certificación cumpliendo todas las obligaciones del primer grupo: Colegio de Arquitectos de Sevilla, IpsCA.
- *Firma electrónica reconocida*, con todas las de la Ley: FNMT, DNle.

- *Firma electrónica (simple)*: conforme a las condiciones acordadas por las partes para relacionarse entre sí. El remite de un email, el pin de una tarjeta de crédito
- *Firma electrónica avanzada*, la que se basa en un sistema de clave pública: PGP, la utilizada en MSWord
- *Firma electrónica avanzada y certificada*, es la que está garantizada por un prestador de servicios, cumpliendo algunas de las obligaciones anteriores: Lefis, CertiVer
- *Firma electrónica basada en certificado no reconocido*, garantizada por un prestador de servicios de certificación cumpliendo todas las obligaciones del primer grupo: Colegio de Arquitectos de Sevilla, IpsCA.
- *Firma electrónica reconocida*, con todas las de la Ley: FNMT, DNle.

- *Firma electrónica (simple)*: conforme a las condiciones acordadas por las partes para relacionarse entre sí. El remite de un email, el pin de una tarjeta de crédito
- *Firma electrónica avanzada*, la que se basa en un sistema de clave pública: PGP, la utilizada en MSWord
- *Firma electrónica avanzada y certificada*, es la que está garantizada por un prestador de servicios, cumpliendo algunas de las obligaciones anteriores: Lefis, CertiVer
- *Firma electrónica basada en certificado no reconocido*, garantizada por un prestador de servicios de certificación cumpliendo todas las obligaciones del primer grupo: Colegio de Arquitectos de Sevilla, IpsCA.
- *Firma electrónica reconocida*, con todas las de la Ley: FNMT, DNIe.

- *Firma electrónica (simple)*: conforme a las condiciones acordadas por las partes para relacionarse entre sí. El remite de un email, el pin de una tarjeta de crédito
- *Firma electrónica avanzada*, la que se basa en un sistema de clave pública: PGP, la utilizada en MSWord
- *Firma electrónica avanzada y certificada*, es la que está garantizada por un prestador de servicios, cumpliendo algunas de las obligaciones anteriores: Lefis, CertiVer
- *Firma electrónica basada en certificado no reconocido*, garantizada por un prestador de servicios de certificación cumpliendo todas las obligaciones del primer grupo: Colegio de Arquitectos de Sevilla, IpsCA.
- *Firma electrónica reconocida*, con todas las de la Ley: FNMT, DNle.

- *Firma electrónica (simple)*: conforme a las condiciones acordadas por las partes para relacionarse entre sí. El remite de un email, el pin de una tarjeta de crédito
- *Firma electrónica avanzada*, la que se basa en un sistema de clave pública: PGP, la utilizada en MSWord
- *Firma electrónica avanzada y certificada*, es la que está garantizada por un prestador de servicios, cumpliendo algunas de las obligaciones anteriores: Lefis, CertiVer
- *Firma electrónica basada en certificado no reconocido*, garantizada por un prestador de servicios de certificación cumpliendo todas las obligaciones del primer grupo: Colegio de Arquitectos de Sevilla, IpsCA.
- *Firma electrónica reconocida*, con todas las de la Ley: FNMT, DNle.

Petición de identificación de usuario




El siguiente sitio ha pedido que usted se identifique con un certificado:

OVAL.MUFACE.ES (:443)

Organización: "FNMT"

Emitido bajo: "FNMT"

Elija un certificado para presentarlo como identificación:

DNI electrónico:CertAutenticacion [61:BE:92:5B:91:27:28:4B:46:96:08:28:BE:76:9E:C0] 

DNI electrónico:CertAutenticacion [61:BE:92:5B:91:27:28:4B:46:96:08:28:BE:76:9E:C0]

DNI electrónico:CertFirmaDigital [44:66:82:6D:A2:90:1B:CA:46:96:08:28:8D:82:3E:03]

(AUTENTICACIÓN)", givenName=MANUEL, SN=VAZQUEZ, serialNumber=17174158N, C=ES

Número de serie: 61:BE:92:5B:91:27:28:4B:46:96:08:28:BE:76:9E:C0

Válido de 12/07/2007 12:53:28 para 12/01/2010 11:53:28

Propósitos: Cliente, Firma

Utilización de la clave de certificado: Firmando

Expedido por: CN=AC DNIE 001, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES

Almacenado en: DNI electrónico

Aceptar

Cancelar

identificación y autenticación

- sistemas conformes a la Ley 59/2003 y admitidos
- por supuesto el DNle
- firma electrónica avanzada (incluyendo los certificados reconocidos y admitidos por la Administración)
- claves concertadas entre la Administración y el ciudadano
- información conocida solo por las partes
- otros sistemas

- Real Decreto 1671/2009, desarrollo parcial de la Ley 11
- Real Decreto 3/2010, por el que se regula el Esquema Nacional de seguridad en el ámbito de la Administración Electrónica
- Real Decreto 4/2010, por el que se regula el Esquema Nacional de interoperabilidad en el ámbito de la Administración Electrónica

sobre otros sistemas de firma electrónica

- La admisión de otros sistemas de firma electrónica a la que se refiere la Ley 11, deberán aprobarse mediante orden ministerial, o resolución del titular en el caso de los organismos públicos, previo informe del Consejo Superior de Administración Electrónica.
- El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación que sean necesarios de acuerdo con la legislación que le sea aplicable.

sobre el Esquema Nacional de Interoperabilidad

- La AGE definirá una política de firma electrónica que servirá de marco general de interoperabilidad para el reconocimiento mutuo de firmas electrónicas
- Las Administraciones públicas aprobarán su política de firma electrónica partiendo de una norma técnica
- La política de firma electrónica establecerá las características de la lista de prestadores de servicios de certificación que recogerá los certificados reconocidos e interoperables entre las Administraciones públicas tanto en el ámbito nacional como europeo

norma técnica sobre firmas electrónicas y certificados

- seguridad y organización,
- características técnicas y legales de generación, verificación y gestión
- características de los certificados y formatos de firma
- algoritmos y longitudes mínimas de las claves
- reglas de creación y validación
- uso de las referencias temporales y de sello de tiempo
- normalización de la representación de la firma electrónica en pantalla y en papel

lo que queda por hacer

- Publicación de la norma técnica y de las políticas de la AGE. Probablemente basada en los estándares internacionales: DPC, ETSI TS x x, PKCS #11 (Laboratories RSA), RFC 3739 Internet X.509, ...
- Ordenar el caos de los prestadores de servicios de certificación (a nivel europeo)
- Confeccionar la lista de servicios de confianza (TSL), de acceso público, que recogerá información precisa y actualizada de aquellos servicios de firma aptos para su empleo en un marco de interoperabilidad de las Administraciones públicas españolas y europeas

y sobre todo ...

¡hay que usar la firma electrónica!