La firma electrónica

JOAQUÍN ROSÉS SANZ
Abogado

La firma electrónica

Joaquín Rosés Sans
Abogado

Jornadas sobre Derecho e Internet

Cáceres
Noviembre
2000

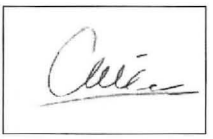
www.abog.net/roses
www.webglass.com/roses

e-mail: jroses@icab.es

Roger de Llúria, 81, 2/1-A
08009 Barcelona
Tel: 93 487 73 73 · Fax: 93 487 73 57

El documento y la firma.

- **Se trata de conceptos no definidos legalmente.**



- **Es de general conocimiento:**
  - Cualquier persona sabe lo que es un documento y lo que es una firma.
  - Se tiene conciencia de la trascendencia del acto de firmar.

La firma manuscrita

- **Es el signo apto para:**
  - dar autenticidad y demostrar la aprobación del contenido de una declaración escrita

    o, dicho de otra manera
  - poderse apreciar como expresión de la voluntad de un sujeto determinado.

25/11/2000 **Joaquín Rosés Sans - Abogado** 3

Doble valor de la firma

La firma es:

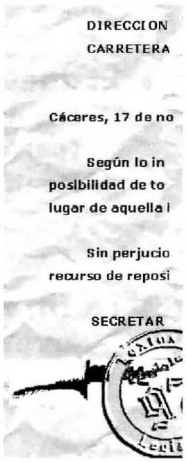
expresión de la voluntad de un sujeto determinado

Alguien en concreto	Está de acuerdo con

25/11/2000 **Joaquín Rosés Sans - Abogado** 4

El documento tradicional

- **Tiene entidad e identidad propios**
- **Es un conjunto formado por:**
  - El papel (soporte físico)
  - Contenido (parte sustantiva)
    - Texto / Datos / Imagenes / Fecha
  - Firma(s) que lo autoritzan
  - Marcas de autenticidada o identificación:
    - Sello(s)
    - Filigranas / Sistemas de impresión
    - Numeración / Códigos
- **Existe un original**


DIRECCION
CARRETERA

Cáceres, 17 de no

Según lo in
posibilidad de to
lugar de aquella i

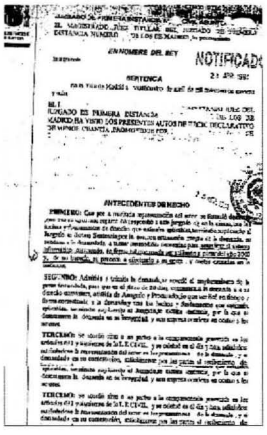
Sin perjucio
recurso de reposi

SECRETAR

25/11/2000 **Joaquín Rosés Sans - Abogado** 5

Características del documento tradicional

- **no necesita medios técnicos especiales**
- **lo asociamos a una determinada imagen**
  de conocimiento general
- **a simple vista lo damos por bueno**
- **confiamos**
  porqué conocemos perfectamente el concepto.
  (incluso de las copias, ya que se pueden contrastar con el original)


EN NOMBRE DEL REY

NOTIFICAD

SENTENCIA

ANTECEDENTES DE HECHO

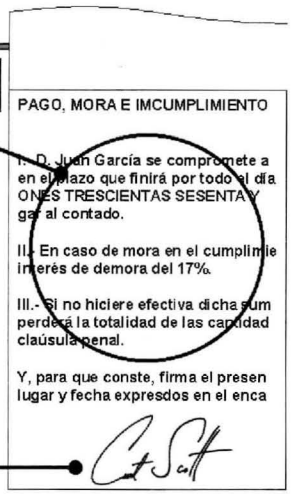
25/11/2000 **Joaquín Rosés Sans - Abogado** 6

El documento firmado

que (contenido)

- **El documento contiene:**
  - **Los datos del/de los firmante/s (partes)**
  - **Manifestaciones y declaraciones (contenido)**
- **La firma estampada en él:**
  - **Aprueba el contenido**
  - **Identifica al/a los firmante/s**

Quien + conformidad


PAGO, MORA E IMCUMPLIMIENTO

I.- D. Juan García se compromete a
en el plazo que finirá por todo el día
ONES TRESCIENTAS SESENTA Y
gar al contado.

II.- En caso de mora en el cumplimie
interés de demora del 17%.

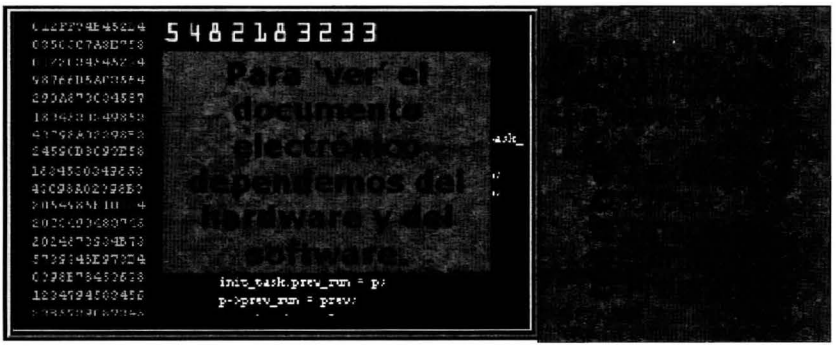
III.- Si no hiciere efectiva dicha sum
perderá la totalidad de las cantidad
claúsula penal.

Y, para que conste, firma el presen
lugar y fecha expresdos en el enca

25/11/2000 **Joaquín Rosés Sans - Abogado** 7

El documento electrónico

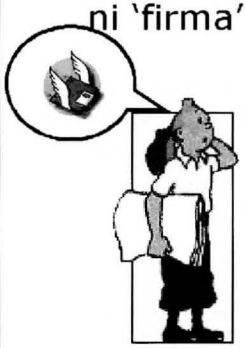
- ¿ Existe el 'documento electrónico' ?
- ¿ Hay un original ? ¿ Hay copias ?

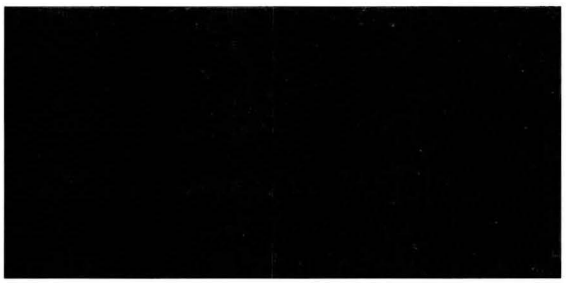


25/11/2000 **Joaquín Rosés Sans - Abogado** 8

Negocio jurídico y documento electrónico.

Si un negocio jurídico se formaliza por medios electrónicos no hay ni 'documento' ni 'firma' tradicionales.





25/11/2000 **Joaquín Rosés Sans - Abogado** 9

La firma electrónica

No de forma absoluta

Es el instrumento técnico que mejor cubre las necesidades de seguriad para:

- Identificar al sujeto.
- Acreditar el contenido del documento (garantizando la integridad)
- Tener eficacia probatoria.

25/11/2000 **Joaquín Rosés Sans - Abogado** 10

Valor jurídico de la firma electrónica.

- El RDL 14/99 le da igual valor jurídico que la firma manuscrita

Equivalencia funcional

- **La firma 'avanzada'** (certificado acreditado):
  - "tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel" y
  - "será admisible como prueba en juicio"
- **La firma no avanzada** (no acreditada):
  - "no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica."

25/11/2000 **Joaquín Rosés Sans - Abogado** 11

Requerimientos de la firma electrónica **para su equivalencia con la manuscrita.**

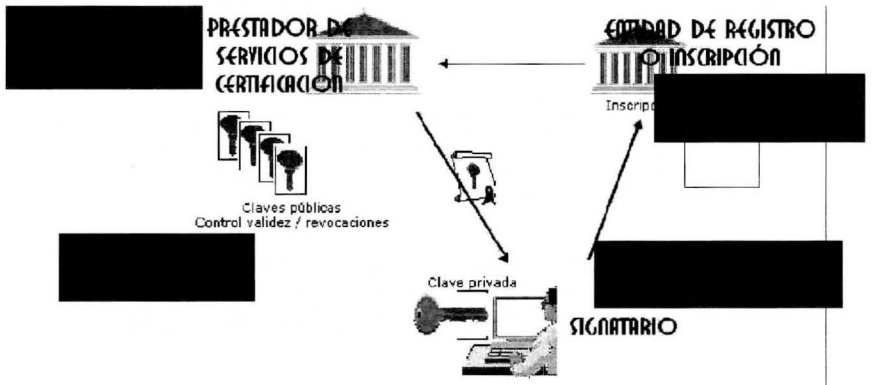
- Se trate de una FE avanzada (identificación del signatario y que permita detectar alteraciones posteriores)
- Esté basada en un Certificado Reconocido (emitido por un PSC: fiabilidad, seguridad, garantía)

Componente tecnológica

- Haya sido generada por un procedimiento seguro (irrepetibilidad, secreto, no falsificable)

25/11/2000 **Joaquín Rosés Sans - Abogado** 12

El tercero de confianza: el Prestador de Servicios de Certificación.



25/11/2000 **Joaquín Rosés Sans - Abogado** 13

Valores añadidos de la firma electrónica.

- La presunción de autenticidad del emisor o autor del mensaje --> garantia de "no repudio"

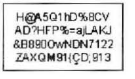
  Se ha identificado + No se puede falsear = Ha sido él

- Integridad:

  Presunciones legales

  Si se altera el documento la firma no es valida
  Por tanto: firma válida = documento íntegro

- Confidencialidad:
  Se puede encriptar = No pueden verlo otros



- Se puede acreditar la fecha y la hora
  Mediante sistemas de *timestamping*

25/11/2000 **Joaquín Rosés Sans - Abogado** 14

Problemas inherentes a la firma electrónica.

- **Dependencia de la tecnología** - ***"Acto de fé" sobre la bondad y seguridad técnica de los sistemas criptográficos.***
- **El usuario no tiene el control ni del hardware ni del software** - ***La firma no depende de la persona, sino de la máquina y los programas usados. Siquiera puede asegurarse que el usuario haya querido firmar.***
- **Pueden darse casos de 'voluntad suplantada' en los que no existirá 'falsedad' en la firma** - ***La firma en si misma será 'auténtica'.***

La presunción legal (art. 3) + garantía prestada por el PSC = Fiabilidad

25/11/2000 **Joaquín Rosés Sans - Abogado** 15

Marco legal de la firma electrónica.

Pero la red si lo és.

- No hay norma 'universal' UNCITRAL Proyecto de régimen uniforme
- Directivas europeas (1999/93/CE de firma electrónica y 200/31/CE de comercio electrónico)
- Normas nacionales.
  - La primera en EEUU, Estado de Utha (1995)
  - En España el RDL 14/1999 de 17/9/99

Normas muy "jóvenes"

- Diversas normas sectoriales:

Normas para cada caso concreto. No se ha asumido aún el concepto con carácter general.

- Ley "Cambiaria y del Cheque" (1985), Reglamento del IVA (Factura telemática), Sistema CIFRADOC de la CNMV, etc
- RD 1906/99, de 17/12/99 "Contratación telefónica o electrónica con condiciones generales de contratación"
- Normas diversas **AEAT** presentación declaraciones fiscales.
- Normas Notariado / Registros de la Propiedad y Mercantiles

25/11/2000 **Joaquín Rosés Sans - Abogado** 16

Marco Legal. Primeros antecedentes.

Normas sectoriales dispersas anteriores al RDL 14/99

Eminentemente de derecho público

- Ley Cambiaria y del Cheque (1985)
- Ley 30/1992 del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común de 1.992, y Decreto 263/1996, 16 de febrero, sobre el uso de la información electrónica, y técnicas telemáticas por parte de la Administración General del Estado
- Orden de 3 de abril de 1.995 sobre uso de medios electrónicos en la Seguridad Social, y normativa de desarrollo del sistema RED, hasta la resolución de 17 de enero de 1.996.
- LORTAD 1992 (hoy Ley Orgánica de Protección de Datos de 1.999)
- Ley y Reglamento del IVA, con referencia a la factura telemática (1.993, 1.996)
- Reglamentación de la CNMV, y del Sistema de Interconexión Bursátil, para la implantación del sistema CIFRADOC-CNMV que contempla el uso de criptografía de clave pública.
- Instrucción de 29 de octubre de 1.996, de la Dirección General de los Registros y del Notariado.

25/11/2000 **Joaquín Rosés Sans - Abogado** 17

Marco Legal. Directiva 1999/93/CE.

por la que se establece un Marco comunitario para la Firma Electrónica,

aprobada por el Parlamento y el Consejo de la Unión Europea el 13 de Diciembre de 1999

- Marco jurídico para los servicios de certificación
- Definición de los requisitos para Europa de los proveedores de servicios y de los certificados
- Promover libre oferta de servicios sin autorización previa
- Permitir la introducción de niveles voluntarios de acreditación
- Promover la validez jurídica de las firmas electrónicas
- Introducir normas sobre responsabilidad
- Introducir mecanismos de cooperación

▶

25/11/2000 **Joaquín Rosés Sans - Abogado** 18

Marco Legal. RDL 14/1999.

Convalidado por Resolución del Congreso de los Diputados de 21/1099

de 17 de Septiembre sobre firma electrónica

- Regulación de su uso y atribución de eficacia jurídica
- Régimen aplicable a los Prestadores de Servicios de Certificación
- Registro de Prestadores de Servicios de Certificación
- Régimen de inspección administrativa de su actividad
- Expedición y pérdida de eficacia de los certificados
- Régimen de infracciones y sanciones que se preven para garantizar su cumplimiento

- La ORDEN de 21/02/2000 aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

25/11/2000 **Joaquín Rosés Sans - Abogado** 19

Marco Legal. RD 1906/1999.

de 17/12/99 por el que se regula la contratación telefónica o electrónica con condiciones generales.

- **Se aplica a contratos:**
  - Con Condiciones General de Contratación (Ley 7/98)
  - Sujetos a la legislación española, o a legislación extranjera cuando el adherente haya emitido su declaración negocial en territorio español y tenga aquí su residencia habitual
  - Celebrados a distancia, o sin presencia física simultánea de los contratantes, realizados por vía telefónica, electrónica o telemática.

- **Carga de la prueba recae en el predisponente. Deberá utilizarse una firma electrónica avanzada con consignación de fecha y hora de remisión y recepción.**

25/11/2000 **Joaquín Rosés Sans - Abogado** 20

Marco Legal . . . . . .

... los conceptos de documento y firma electrónicos, así como otros propios de las nuevas tecnologías, deben ser socialmente asumidos y adquirir la condición de usuales. Un día las normas legales ya no deberán regularlos más allá de lo que hoy regulan el documento o la firma 'tradicionales', el teléfono, el automóvil . . . conceptos que en su día fueron también novedosos y carecían de previsiones legales.

25/11/2000 **Joaquín Rosés Sans - Abogado** 21

Aplicaciones de los certificados digitales (firma electrónica).

- Firmado de emails
- Autentificación de usuarios
- Autentificación de webs
- Firma de mensajes en sistemas EDI, SET, etc

- Firma de documentos de texto, imágenes (planos, proyectos)...
- Firma de programas, de música, vídeo ...
- Identificación entre partes desconocidas.

25/11/2000 **Joaquín Rosés Sans - Abogado** 22

Ejemplos de aplicaciones de F.E. (1)

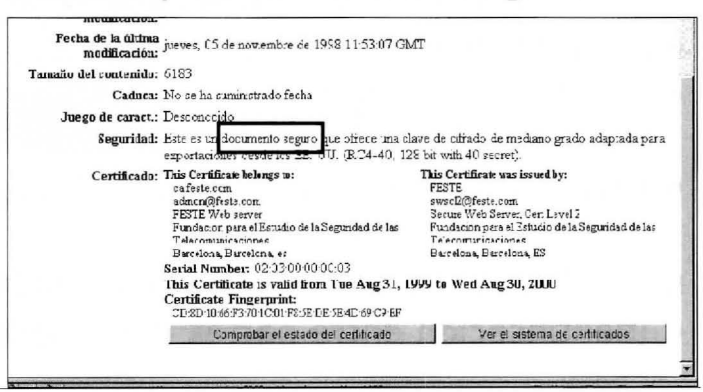
Firmado de correo electrónico:

- Identidad
- Autenticidad
- Integridad

Ejemplos de aplicaciones de F.E. (2)

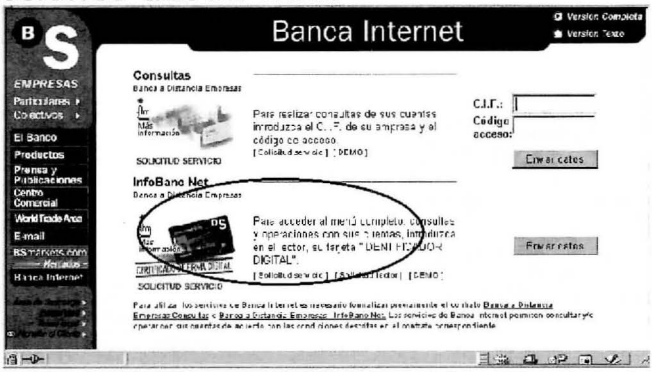
Autentificación de sitios web:

- Identidad y Autenticidad = seguridad



Ejemplos de aplicaciones de F.E. (3)

Autentificación (control de acceso) de usuarios y firmado de los mensajes en transacciones desde web.



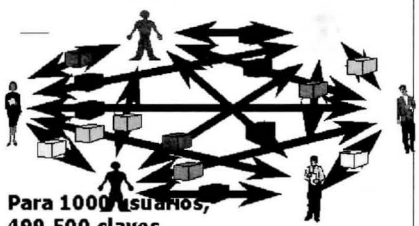
Criptografía. La base de la F.E. (1)

- La firma electrónica se basa en procesos criptográficos (cifrado, encriptación).
- Se utiliza el sistema de doble clave asimétrica (privada / pública) e interviene un 'tercero confiable', que: identifica al signatario y custodia las claves públicas (y sus revocaciones).

Criptografía. La base de la F.E. (2)

Clave simétrica:

- La misma para cifrar y para descifrar
- Se necesita una clave para cada interlocutor.



Para 1000 usuarios, 499.500 claves

Clave asimétrica:

- Una clave para cifrar y otra distinta para descifrar
- Una sola clave sirve para todos los interlocutores.

Para 1000 usuarios, 1.000 claves

25/11/2000 **Joaquín Rosés Sans - Abogado** 27

Criptografía. La base de la F.E. (3)

Algoritmo RSA:

- Se toman dos números primos, "**p**" y "**q**" grandes (de unos 100 dígitos cada uno)
- Se hace **n=p·q** (uno de los componentes de las claves)
- Se calcula **Ø=Ø(n)=(p-1)·(q-1)** (función de Euler).
- Se seleccionan dos números "**e**" y "**d**", uno de ellos primo (al menos respecto a "**Ø**") tomado del intervalo **(max(p, q)+1, n-1)**, de forma que se cumpla **e·d= 1 mod Ø**, es decir, *tal que exista un número racional "t" que haga* ***e·d=Ø·t+1***. Dicho de otra forma, "**e**" y "**d**" cumplen la propiedad de ser *inversos* ***mod Ø***
- **Tras este proceso, tenemos "n", "e" y "d".**
- **Las claves son (n,e) y (n,d)**

Conociendo "Ø" es fácil calcular "e" a partir de "d" y viceversa. Sin embargo, para conocer "Ø" es necesario conocer "p" y "q", lo que exige factorizar "n".

25/11/2000 **Joaquín Rosés Sans - Abogado** 28

Criptografia. La base de la F.E. (4)

Ejemplo del algoritmo RSA:

- Tomamos **p=5** y **q =11** primos, por lo que obtenemos **n=5·11=55**.
- De ahí, **Ø=Ø(n)=4·10=40** (que factorizándolo da **Ø=5·2^3**).
- Podemos tomar **e=23 (entre 12 y 33** sin factores comunes con "**Ø**")
- Para encontrar "**d**", operamos: **d=(Ø·t+1)/e**, es decir, **d=(40·t+1)/23**. Con **t=4** vemos que **d=7**.
- **Así que una clave es (7,55) y la otra (23,55).**
- *Para **cifrar** se eleva el dato a la potencia de (**7 o 23**, elegir uno). El resultado lo dividimos por **55. El** resto es el **criptograma**.*
- *Para **descifrar**, se eleva el criptograma a a la potencia de (**23 o 7**, elegir el **distinto** del de cifrar). Dividimos por **55. El** resto es el **dato original**.*

*Si ciframos "**2**", 2^7 mod **55** = **18**;*
*Para descifrar: 18^{23} mod **55** = **2***

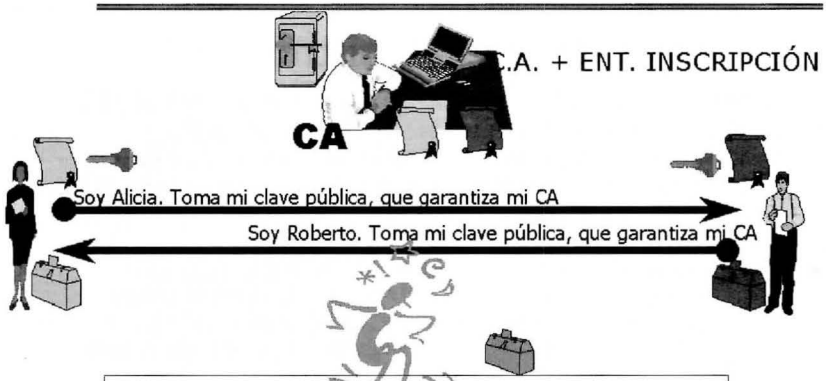
25/11/2000 **Joaquín Rosés Sans - Abogado** 29

La necesidad del tercero confiable (1)

Sin intervención de tercero no se acredita la personalidad. Puede haber suplantación.

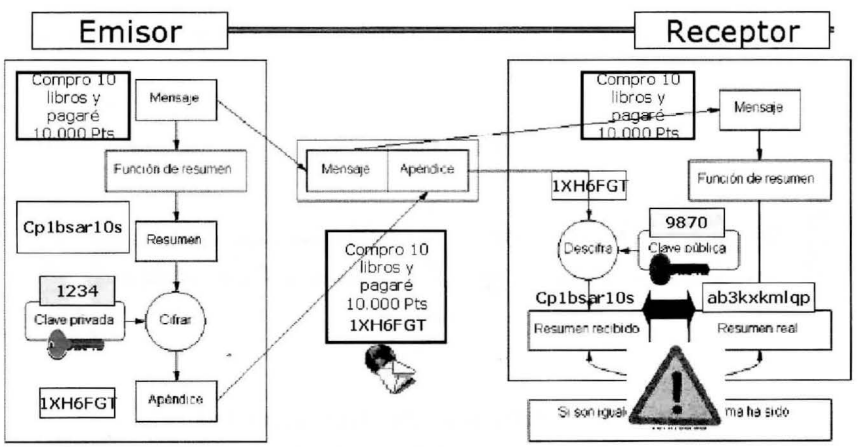
25/11/2000 **Joaquín Rosés Sans - Abogado** 30

La necesidad del tercero confiable (2)



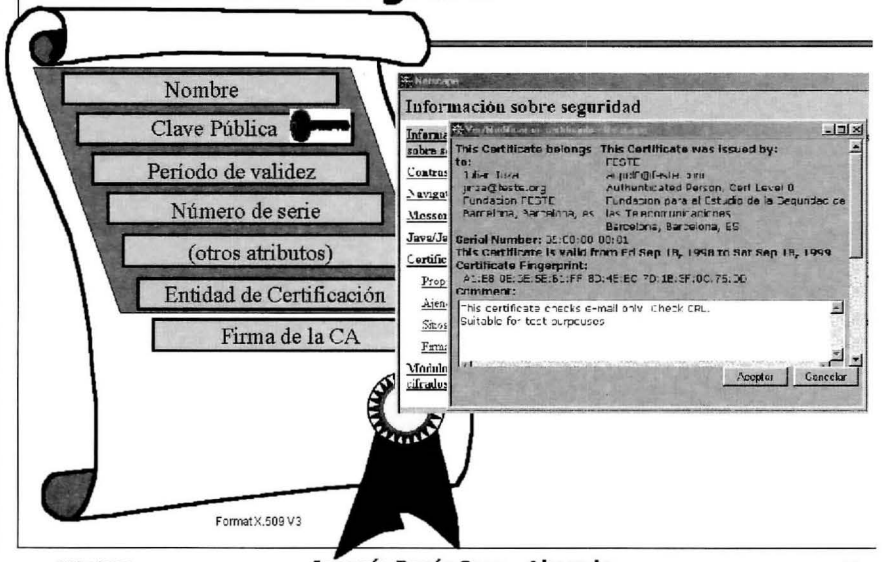
Con la intervención de un tercero de confianza se acredita la personalidad.
No puede haber suplantación.

Proceso de firma y de verificación.



El proceso es automático y "transparente" para el usuario

El certificado digital.



25/11/2000 **Joaquín Rosés Sans - Abogado** 33

Seguridad técnica, confianza y valor legal.

- La seguridad reside en la técnica (criptografia y medidas de seguridad)
- La confianza la aportan los terceros intervinientes (CA y EI)
- La "garantía" viene dada por la Ley, que da validez a la firma electrónica, y prevé sistemas de aseguramiento.

25/11/2000 **Joaquín Rosés Sans - Abogado** 34