



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

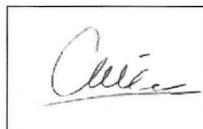
25/11/2000

Joaquín Rosés Sans - Abogado

1

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.



25/11/2000

Joaquín Rosés Sans - Abogado

2

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 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 INCUMPLIMIENTO

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

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

III.- Si no hiciere efectiva dicha suma perderá la totalidad de las cantidad cláusula penal.

Y, para que conste, firma el presente lugar y fecha expresados en el enca

Cat Salt

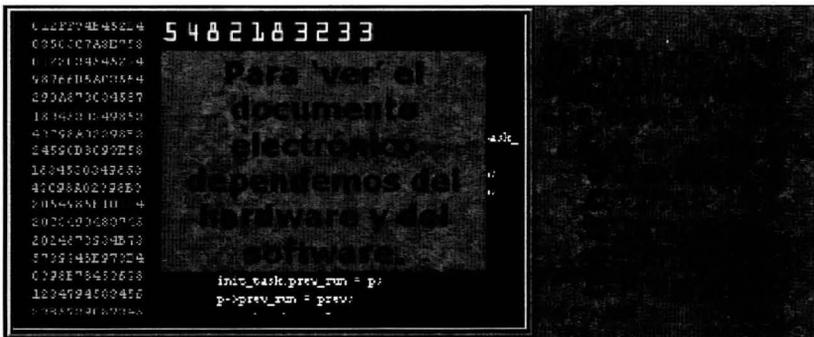
25/11/2000

Joaquín Rosés Sans - Abogado

7

El documento electrónico

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



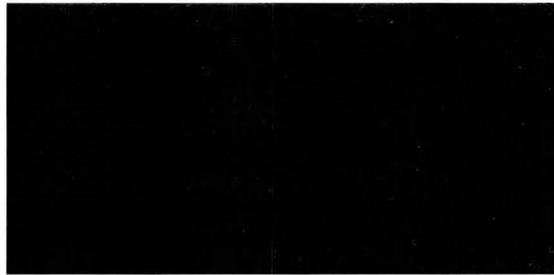
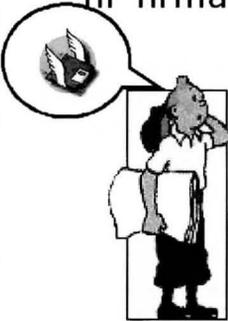
25/11/2000

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

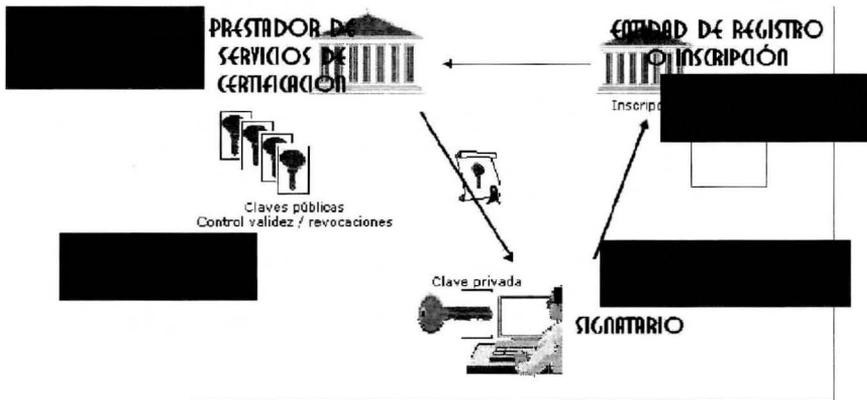
Componente tecnológica

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 --> garantía 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 válida
Por tanto: firma válida = documento íntegro



- Confidencialidad:
Se puede encriptar = No pueden verlo otros

```
H@a5011D%8CV
AD7FFP%ajLAKJ
&B880wNDN7122
ZAXQM9H1çD,813
```

- 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
- **Diversas normas sectoriales:**

Normas muy "jóvenes"

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

- Ley "Cambiaría 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

- 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 CIFRADO-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.

Eminentemente de derecho público

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

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
- Autenticación de usuarios
- Autenticación 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



25/11/2000

Joaquín Rosés Sans - Abogado

23

Mensaje de Notepad

Archivo Edición Ver Signatures Mensaje Comunicador Ayuda

```
-----_NextPart_00E_0000_01BE6C9D.DC9DA180
Content-Type: application/x-pkcs7-signature;
name="smlenc.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="smlenc.p7s"
```

```
MFACCSqRSTh3DQFHaqPAMIAcaQExCz6.JgItr3gMCSGUAHAGESqRSTh3DQFHAQAAo1IHXJCCa3ku
ggKfAgEAMH6ECSqOsIb3DQCEBBAUHF1Bhngsw0QYU0Q0EwJfUzESHBAGAUUECBHJQmfYV2Us25h
PFI1eAV0UQKULCvXJZk000bEStDKKqgNB8oIQ21b0AR21v0L3wYzJhIC0sIEUz0HWs08q
zUGDQeUz0NcXpCqR1KEL1USX0JRUWVXV1V2V0VpV2Fj3MPLz0XKZP8G9MHS1IHX13UdL
bnRpV2F0ZUgU0gY29ULCBZ2J0IEX1Lw0s1DaxDjAHBgnUEARtBU2FUFRFR8v0YJkoZ1huc
nQKf8hndXBj0B0zWz0CUvZ0VMB0XKt0NDVvN1E3NDgyM1axDTILw0MHE1E3NDgyM0w0g0E
E2zJgN0BvY1F8I1N1ULFYU0U1EwJ0XJjZk000bEXjR0UgM0B8c1C0JncMHD69Y1I1H0K0E
A1UE0AH0R0u0GfjAM01H0c0EgZ0wJRH0d8p0b0C250sY81Z0d0c1kV0MgZ0Ug0fCFRL
b0Uj0211b0LjV0M0s251c0Eh0C0d0A1UEEM1QX00a0Ud0C1jVX01Z0B0Z0J0b20cIF01c0G0f0C0Z
ZV0gT0E0M0w0R10E0x0F0K0IUL0XhZ0d0g0k01E0V0M0CJ0E0W010C0NS0M0B0z0XN0SjE20g0a1u
DQYJkoZ1hucN6QC0B0d0g0A0H1B0H0D0E0V0T1E0A0z0V0W0U0g0f0C0I0g0E0V620Y0g070s1nc0t
P1nc0H1J0g0R0B0Z0U0F0P0E0S0A0R0E1J050x0F0H0B0R07E0J0h0E0y0B0A0C0Z1C0D0p0z690M0g0
1G0K1F0N0z0U0AM0Z0B0CS0S0Y0M0U0S0X0D0M0X000M0V20U0M0Z0S0K0V0U0D0L0E0B0C0R0Z0V
0A0H0d0K0IF01C0h0b10g0Z0Ug0D0E2K21C0A0W0Q040v0V0Q0C0W0R0U0R1C1F0D0C0S0G0S1B0D0E0J
AR0VZ0u0V20w0C21c0R1L0w0B0Q1F0Q0A0D0M0C0V0K0u0A0h0F0K0C0A0E0G0VJkoZ1hucN6KQ0d0Q0c
CS0E51D0D0E0T0c0g0q0h1E090B0C0U0X0c0D0T0W01Y0V01T1Wj0J0k0h0k150W0B0C0Q0x070U
S0f0e0e20v0H0E0e0ST0C01nc0h0w0JkoZ1hucN6KQ0d0Q0c1E0V0M0CJ0E0W010C0NS0M0B0z0XN0SjE20g0a1u
Dg0Cj0K0B0g0h0c090w0B0C0T0R0AV0J0w0V0B0A0C0W0E0M0H0H0I0N0H0D0E0C0V0D0Q0C0E0JF1E2S0W0A0
A1UE0M1J0Q0F0Y20s0z50H0E10E0V0D0U0H0L0V0ZjZ0x0b0E0X0D0R0q0N0B0u1QZ10m0R0Y210u10u
V0Jh1C0U0IEUz0H010M0g0Z0Ug0C0Eg0U0d0Xp20FjC0R1J0C0h0c0Y0U20W1V290d0Y0p2Fj0w0V20X0B
R0R0g0N0B0s1I0f10d0Th0R0Y2F0W0g0U0y020U1C0D0Z0L0F01d0w01D0x0JAH0B0E0A0H0R1Z0
U0R1F0B0H0Y0R0C10w0h0V0F0B0X0Ej0B0Z0V0d0U0V20L0q0F0A0M0H0A0B0q0h1K0S0W0B0E0F
0AR0V0Q0h1D0c0N0Y0E0g0T0g0w0pLJL0P0X0K0A0J0S0J0070C0D0H0K0C0E0T0N011F0A00R0u000
m00F070m0W0jF0Q0A0A0A0A0A0=
```

-----_NextPart_00E_0000_01BE6C9D.DC9DA180-----

Ejemplos de aplicaciones de F.E. (2)

Autenticación de sitios web:

- Identidad y Autenticidad = seguridad

Fecha de la última modificación: jueves, 05 de noviembre de 1958 11:53:07 GMT
Tamaño del contenido: 6183
Caduce: No se ha especificado fecha
Juego de caract.: Desconocido
Seguridad: Este es un documento seguro que ofrece una clave de cifrado de mediano grado adaptada para espionaje. Ver el artículo 11.3.5 U.S. (R.24-40, 126 bit with 40 secret).

Certificado: This Certificate belongs to:	This Certificate was issued by:
ca.feste.com	FESTE
adenc@feste.com	adenc@feste.com
FESTE Web server	Secure Web Server, Cert. Level 2
Fundador para el Estudio de la Seguridad de las Telecomunicaciones	Fundacion para el Estudio de la Seguridad de las Telecomunicaciones
Buenos Aires, Buenos Aires	Buenos Aires, Buenos Aires

Serial Number: 02320000000000
This Certificate is valid from Tue Aug 31, 1999 to Wed Aug 30, 2000
Certificate Fingerprint: C1E8D1046F37D1C01FE3E0E5E4C69C9EF

25/11/2000

Joaquín Rosés Sans - Abogado

24

Ejemplos de aplicaciones de F.E. (3)

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

The screenshot shows the 'Banca Internet' interface. On the left is a navigation menu with options like 'EMPRESAS', 'El Banco', 'Productos', 'WorldWide Area', 'E-mail', 'BS Internet', and 'Navegación'. The main content area is titled 'Consultas Banca a Distancia Empresas' and contains two sections: 'InfoBanco Net' and 'InfoBanco Web'. The 'InfoBanco Net' section is circled in red and includes a form with fields for 'C.I.F.' and 'Código acceso', and a 'Enviar datos' button. The 'InfoBanco Web' section includes a form with a 'Código de acceso' field and a 'Enviar datos' button. At the bottom of the page, the text '25/11/2000' is on the left, 'Joaquín Rosés Sans - Abogado' is in the center, and '25' is on the right.

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.



Clave asimétrica:

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



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 $n = p \cdot q$ (uno de los componentes de las claves)
- Se calcula $\phi = \phi(n) = (p-1) \cdot (q-1)$ (función de Euler).
- Se seleccionan dos números "e" y "d", uno de ellos primo (al menos respecto a " ϕ ") tomado del intervalo $(\max(p, q) + 1, n - 1)$, de forma que se cumpla $e \cdot d = 1 \pmod{\phi}$, es decir, tal que exista un número racional "t" que haga $e \cdot d = \phi \cdot t + 1$. Dicho de otra forma, "e" y "d" cumplen la propiedad de ser inversos $\pmod{\phi}$
- Tras este proceso, tenemos "n", "e" y "d".
- Las claves son (n,e) y (n,d)

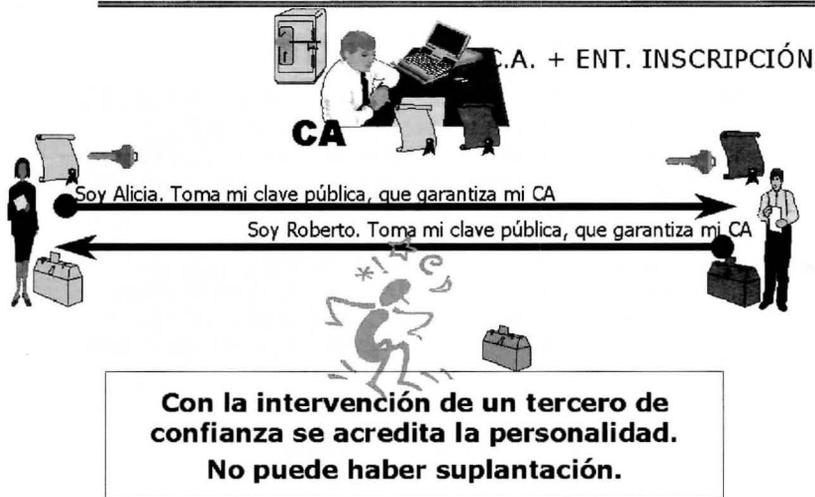
Conociendo " ϕ " es fácil calcular "e" a partir de "d" y viceversa. Sin embargo, para conocer " ϕ " es necesario conocer "p" y "q", lo que exige factorizar "n".

25/11/2000

Joaquín Rosés Sans - Abogado

28

La necesidad del tercero confiable (2)

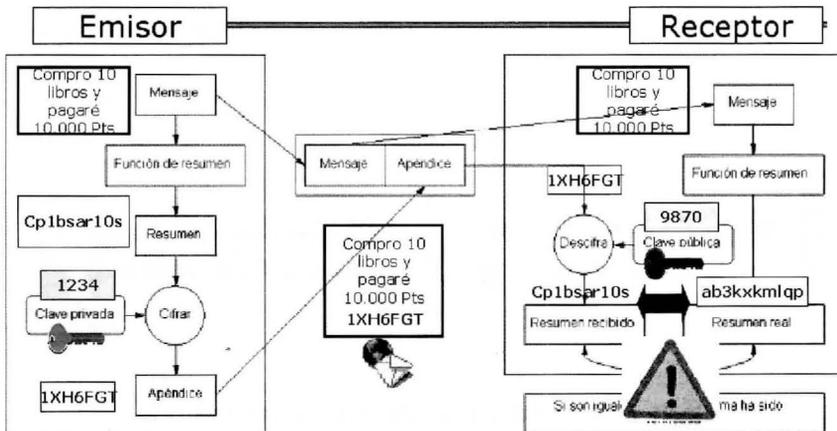


25/11/2000

Joaquín Rosés Sans - Abogado

31

Proceso de firma y de verificación.



El proceso es automático y "transparente" para el usuario

25/11/2000

Joaquín Rosés Sans - Abogado

32

El certificado digital.

The diagram on the left shows a scroll representing a digital certificate with the following fields:

- Nombre
- Clave Pública
- Periodo de validez
- Número de serie
- (otros atributos)
- Entidad de Certificación
- Firma de la CA

Below the scroll is the text "FormatX.509 V3". To the right is a screenshot of a browser security warning window titled "Información sobre seguridad". The window displays the following information:

- Información:** This Certificate belongs to: This Certificate was issued by:
 - to: TIRSA ROSA
 - Organization: joaquinroses.org
 - Common Name: Fundacion FICOTE
 - Location: Barcelona, Spain
 - Country: ES
- Serial Number:** 20:00:00 00:01
- Valid From:** Fri Sep 18, 1998 to Sat Sep 18, 1999
- Certificate Fingerprint:** A2:EB:0E:3E:5E:61:FF:BD:4E:EC:7D:1B:5F:0C:75:0C
- Comments:**
 - This certificate checks e-mail only. Check CRL.
 - Subtitled for test purposes.

At the bottom of the screenshot are "Aceptar" and "Cancelar" buttons.

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

Seguridad técnica, confianza y valor legal.

- La seguridad reside en la técnica (criptografía 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.

