

Sabadell Universitat
Sabadell, 10 de juliol de 2002

***“Marc normatiu i
problemàtica jurídica de la
coordinació electrònica entre
administració i empreses”***

Apol·lònia Martínez Nadal

Professora Titular de Dret Mercantil (UIB)

Directora de l'Àrea jurídica del CEDIB

I.- Introducción: firma, certificados y entid. de cert.

II.- Problemática jco-mercantil de la utilización de la firma electrónica en las relaciones administración-empresas

-Certificados de atributos

-Certificados de persona física-jurídica; esp.ref. al BALFE

-E-DNI

III. El no rechazo en destino: e-notificaciones y acuse de recibo

IV. Reflexiones sobre el futuro de la firma electrónica en la E-administración (AaE)

Introducción

1.- Comunicación electrónica: imposibilidad de firma manuscrita; riesgos:

- a) autenticación**
- b) integridad**
- c) confidencialidad**
- d) no rechazo**

**Exigencias jco-admi.: Ley 30/92 (art. 45)y
RD 263/1996 (art. 4 y 7)**

Introducción

Art. 45.5 Ley 30/92 (*Incorporación de medios técnicos*):

"Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por éstas u otras Leyes".

Introducción

1.- Comunicación electrónica: imposibilidad de firma manuscrita; riesgos

2.- Solución técnica: firma digital, certificados y autoridades de certificación

3.- Cobertura legal:

-RDL 14/1999 de *17 de septiembre*

--desarrollo: OM 20/2/2000

-BALFE

Firma digital (cript. asim.)

A

B

$$M \xrightarrow{K_{SA}(M)} K_{PA}(K_{SA}(M)) = M$$

$K_{SA}(M)$ = mensaje **firmado** con la clave privada (secreta) de A

$K_{PA}(K_{SA}(M))$ = **verificado** con la clave pública de A del mensaje **firmado** con la clave privada de A

Efectos: a) **autenticación**

b) **integridad**

c) **confidencialidad**

d) **no rechazo en origen**

Pendiente: **rechazo en destino**

Firma digital + certificado

Firmas digitales: firmas seguras

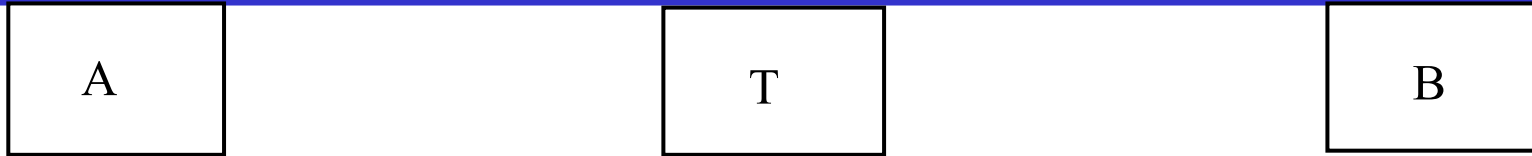
En comunidades amplias, **problema de identificación:**

si A y B son partes desconocidas y geográficamente distantes, no seguridad sobre su identidad (quien dice ser A puede ser realmente un tercero T suplantador)

Solución técnica, y legal: sistema de **certificados**

emitidos por TTPs (p.s.c.) que *vinculan* de forma segura una clave pública, e indirectamente su correspondiente clave privada a una persona determinada

Firma digital + certificado



CA = **certificado** expedido por T

$$K_{PT}(CA) = A, K_{PA}, T_A$$

$$K_{PA}(K_{SA}(M)) = M$$

$K_{SA}(M)$ = mensaje firmado con la clave privada de A

$K_{PT}(CA)$ = verificado con la clave pública de T del certificado

$K_{PA}(K_{SA}(M))$ = verificado con la clave pública de A del mensaje
cifrado con la clave secreta de A

Artículo 8. *Requisitos para la existencia de un certificado reconocido*

- a) La indicación de que se expiden como tales.
- b) El código identificativo único del certificado.
- c) La identificación del prestador de servicios de certificación que expide el certificado,...
- d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra *circunstancia personal del titular*,...
- f) En los supuestos de *representación*, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona (f. o j) a la que represente.
- g) Los datos de verificación de firma que correspondan a los datos de creación de firma ...
- h) El comienzo y el fin del *periodo de validez* del certificado.
- i) Los *límites de uso* del certificado, si se prevén.
- j) Los *límites del valor de las transacciones* para las que puede utilizarse el certificado, ...

Artículo 8. *Requisitos para la existencia de un certificado reconocido*

- a) La indicación de que se expiden como tales.
- b) El código identificativo único del certificado.
- c) La identificación del prestador de servicios de certificación que expide el certificado,...
- d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- e) La *identificación del* signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra *circunstancia personal del titular,...*

BALFE: art. 17: “la **identificación** de los solicitantes de certificados reconocidos exigirá su **personación** ante las personas encargadas de verificar su identidad ...”

Artículo 8. *Requisitos para la existencia de un certificado reconocido*

- a) La indicación de que se expiden como tales.
- b) El código identificativo único del certificado.
- c) La identificación del prestador de servicios de certificación que expide el certificado,...
- d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra *circunstancia personal del titular*,...
- f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona (f. o j) a la que represente.
- g) Los datos de verificación de firma que correspondan a los datos de creación de firma ...
- h) El comienzo y el fin del *periodo de validez* del certificado.
- i) Los límites de uso del certificado, si se prevén.
- j) Los *límites del valor de las transacciones* para las que puede utilizarse el certificado, ...

Certificate:

Data:

Version: 0 (0x0)

Serial Number:

02:41:00:00:16

Signature Algorithm: MD2 digest with RSA Encryption

Issuer: C=US, O=RSA Data Security, Inc.,

OU=Commercial Certification Authority

Validity:

Not Before: Fri Nov 4 10:58:34 1994

Not After: Wed Nov 3 10:58:34 1999

Subject: C=US, O=RSA Data Security, Inc.,

OU=Commercial Certification Authority

Subject Public Key Info:

Public Key Algorithm: RSA Encryption

Public Key:

Modulus:

00:a4:fb:81:62:7b:ce:10:27:dd:e8:f7:be:6c:6e:
c6:70:99:db:b8:d5:05:03:69:28:82:9c:72:7f:96:
3f:8e:ec:ac:29:92:3f:8a:14:f8:42:76:be:bd:5d:
03:b9:90:d4:d0:bc:06:b2:51:33:5f:c4:c2:bf:b6:
8b:8f:99:b6:62:22:60:dd:db:df:20:82:b4:ca:a2:
2f:2d:50:ed:94:32:de:e0:55:8d:d4:68:e2:e0:4c:
d2:cd:05:16:2e:95:66:5c:61:52:38:1e:51:a8:82:
a1:c4:ef:25:e9:0a:e6:8b:2b:8e:31:66:d9:f8:d9:
fd:bd:3b:69:d9:eb

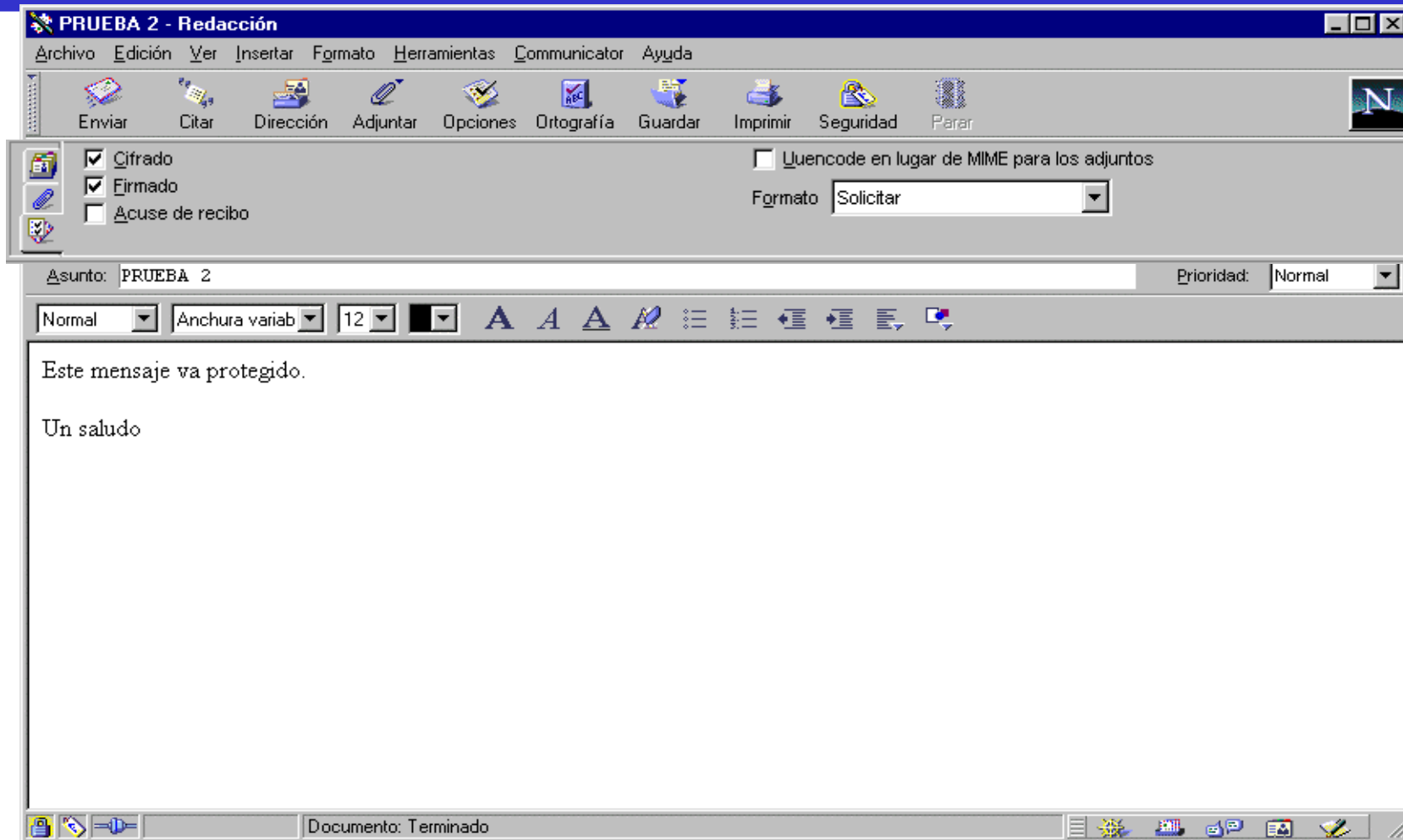
Exponent: 65537 (0x10001)

Signature Algorithm: MD2 digest with RSA Encryption

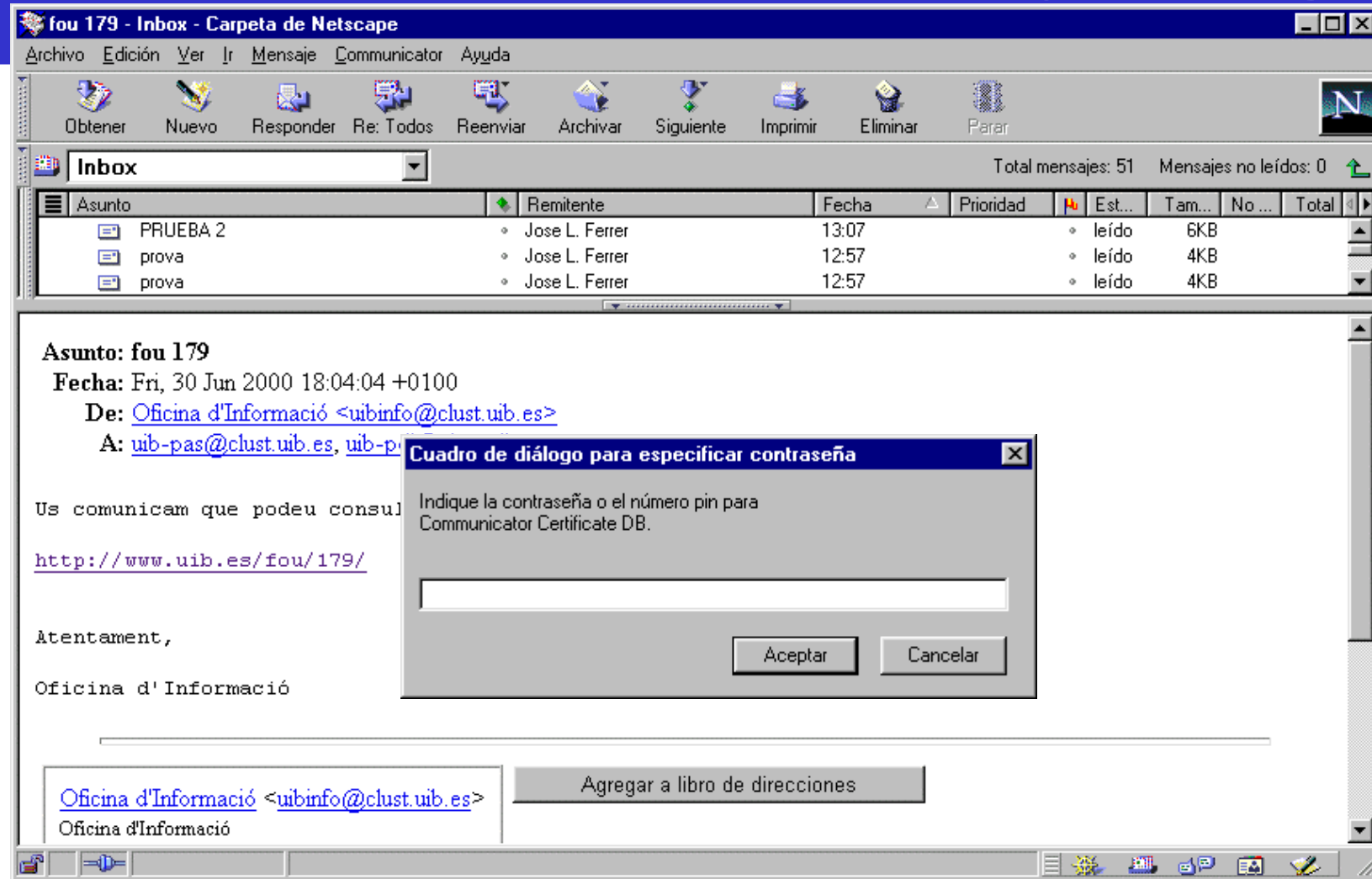
Signature:

76:b5:b6:10:fe:23:f7:f7:59:62:4b:b0:5f:9c:c1:68:bc:49:
bb:b3:49:6f:21:47:5d:2b:9d:54:c4:00:28:3f:98:b9:f2:8a:
83:9b:60:7f:eb:50:c7:ab:05:10:2d:3d:ed:38:02:c1:a5:48:
d2:fe:65:a0:c0:bc:ea:a6:23:16:66:6c:1b:24:a9:f3:ec:79:
35:18:4f:26:c8:e3:af:50:4a:c7:a7:31:6b:d0:7c:18:9d:50:
bf:a9:26:fa:26:2b:46:9c:14:a9:bb:5b:30:98:42:28:b5:4b:
53:bb:43:09:92:40:ba:a8:aa:5a:a4:c6:b6:8b:57:4d:c5

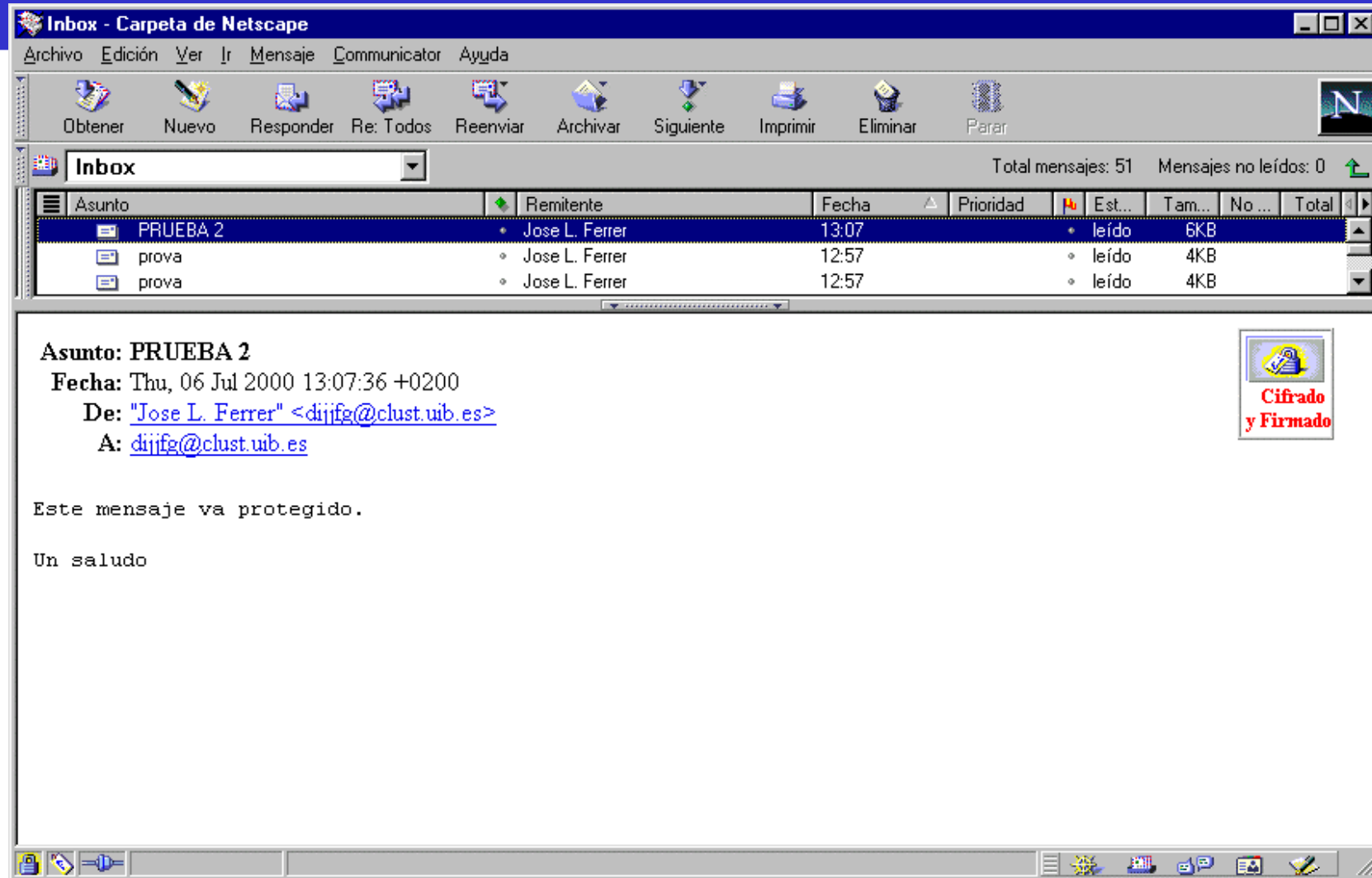
Envío de Mensaje Seguro



Recepción de Mensaje Seguro



Mensaje Seguro (¿?)



Introducción

1.- Comunicación electrónica: imposibilidad de firma manuscrita; riesgos

2.- Solución técnica: firma digital, certificados y autoridades de certificación

**3.- Regulación legal:
RDL 14/1999 (BALFE)**

Cuestiones jco-mercantiles de la firma electrónica en e-AaE

1.- Certificados de atributos

2.- Certificados de pf-pj

3.- E-DNI

1. Certificados de atributos

Concepto general de certificado en el mundo electrónico:

Documento electrónico que contiene una información a la que se ha fijado una firma digital por una entidad reconocida.

Clases:

1.- Certificado de clave pública (identificativo): vinculación clave pública y persona determinada

certificación electr. que vincula unos datos de verificación de firma a un signatario y confirma su identidad (art. 2.5 RDL 14/99).

2.- Certificado de atributos

Certificados que, junto con clave pública e identidad, incluyen cualidad, *característica*, título o poder del titular

Certificado de atributos: función

Función: Incorporación de facultades de representación en el comercio electrónico (poderes, cargos, ...) u otros atributos (títulos, habilitaciones profesionales, etc.)

Solución a la vinculación de personas jurídicas en el mundo electrónico.

Formas de vinculación de persona jurídica:

A) titular del certificado: pf con poder de rptación de la pj

B) titular del certificado: persona jurídica

C) titular del certificado: pj + campo con pf autorizada

Certificado de atributos: rec. legal

1) Derecho español: art. 8 RDL 14/1999:

e) La *identificación del* signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular,....

f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona (f. o j) a la que represente.

2) Reconocimiento técnico: standard X.509 v. 3: extensiones

Cuestiones:

Autorización de la persona representada (no d.español)

Legitimación para revocar de la pers. rptada (art. 9 RDL)

A. Responsabilidad en caso de atributos dinámicos

A) Responsabilidad por la *exactitud inicial* en el momento de la emisión (art. 11.a RDL 14/99): comprobación identidad+otros elementos pers.

B) ¿Resp. por exactitud durante la *vigencia posterior*?

-Art. 6.1.a Dir. Firma el.: responsabilidad “de la veracidad, en el momento de su expedición, de toda la información contenida en el certificado reconocido”.

-Obligación de notificación de cambio por parte del titular

-¿Obligación de la e.c.? (obligación legal/contractual voluntaria)

□ B. El problema de la discordancia con el RM

Divergencia entre el contenido del certificado (y el *Registro de certificados del psc*) y el RM respecto de la existencia, subsistencia y extensión del poder: p.ej., revocación del poder en RM pero no revocación del certificado.

Problema: ¿primacía de otros registros de superior eficacia legalmente reconocida?: caso de poder revocado en RM pero no en Registro del psc:
-en principio, *prevalencia* de realidad del RM sobre apariencia extraregistraral
-no obstante, *el problema del art. 9.2 y 3 del RDL 14/1999:*

Artículo 9: Vigencia de los certificados

1. Los certificados de firma electrónica quedaran sin efecto, si concurre alguna de las siguientes circunstancias:

a) **Expiración** del periodo de validez del certificado.(certificados reconocidos, no superior a cuatro años)

b) **Revocación** por el signatario, por la persona física o jurídica representada por este o por un tercero autorizado. (...)

f) Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, **terminación de la representación** o extinción de la persona jurídica representada (...)

2. La **pérdida de eficacia** de los certificados, en los supuestos de expiración de su periodo de validez y de cese de actividad del prestador de servicios, tendrá lugar **desde que estas circunstancias se produzcan**. En los **demás casos**, la extinción de la eficacia de un certificado surtirá **efectos desde la fecha en que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados** al que se refiere el artículo 11.e).

3. En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en el Registro al que se refiere el artículo 11.e), y responderá de los posibles perjuicios que se causen al signatario o a terceros de buena fe, por el retraso en la publicación. Corresponderá al prestador de servicios la prueba de que los terceros conocían las circunstancias invalidantes del certificado.

Propuestas de solución

I. Solución ideal: coordinación absoluta por vinculación de ambos registros.

P.ej., anotación marginal en RM de emisión de certificado de atributo de administrador; de tal forma que, cuando se quiera inscribir en el RM el cese del administrador, se exigirá previamente la revocación del corresp.certificado.

Crítica: vinculación legal gral.: excesiva; medidas legisl.

Vinculación contractual no gral. (certificados relevantes)

Propuestas de solución

I. Solución ideal: coordinación absoluta por vinculación de ambos registros.

II. Solución de coordinación indirecta: de la legitimación a la carga u obligación de revocar (en especial, del rptado)

a.-Titular

b.-PSC

c.-Representado: legitimación/obligación:

-no derecho español: no consentimiento de pers. rptda

-sí dcho. comparado: p.ej., Ley alemana : consentimiento de pers.rptda (sistema legal permite atribuir obligación)

Propuesta de solución en particular

Prop.de modificación del art. 8.1, f) RDL 14/99 (o desarrollo) para la coordinación indirecta vía obligación del rptado.

f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona (f. o j) a la que represente, cuyo consentimiento será necesario para la emisión del correspondiente certificado.

Tanto el representante como el representado tendrán la obligación de solicitar la revocación del correspondiente certificado en el supuesto de modificación o extinción de la representación que en él constare como atributo”

Conclusión

- Certificados de atributos como elemento de incorporación de las facultades de los apoderados a efectos de firma electrónica.**
- Conveniencia, pese a su problemática.**
- Solución al problema de la discordancia**
 - vía coordinación informática (voluntaria)**
 - o por coordinación indirecta por obligación del rptado de revocar (reforma legislativa)**

Cuestiones

1.- Certificados de atributos

2.- Certificados de pj

3.- E-DNI

2. Certificados de p.j.

Art. 10 BALFE:

“1. Podrán solicitar certificados a favor de personas jurídicas sus administradores, representantes legales y apoderados con poder bastante a estos efectos. ...

2. El uso de los datos de creación de firma y de los certificados reconocidos expedidos a nombre de personas jurídicas corresponderá a una sola persona por certificado, cuyo nombre y apellidos figurarán en el certificado emitido a nombre de la persona jurídica”

Solución de certificado de pj + campo de pf

Cuestiones

1.- Certificados de atributos

2.- Certificados de pj

3.- E-DNI

3. E-DNI

BALFE:

1.- Reformas de la legislación vigente:

- comprobac. previa a la emisión de cert. rec.
- circunstancias y forma de revocación de cert.
- responsabilidad de los psc
- eficacia de la f.el. en entornos cerrados

2.- Novedades:

- DNI electrónico
- certificados de persona jurídica

3. BALFE: E-DNI (art. 6 y 7)

+ válido para usos admi. generales (art. 6.3, pfo.2)

¿-?: ¿otros usos?

“tarjeta equivalente al DNI actual, ...que podrá ser utilizada en las relaciones con cualquier Administración y con los particulares y *empresas*”

(<http://www.setsi.mcyt.es/novedad/firma271201.html>)

¿compatibilidad con principios comunitarios? (art. 6)

¿competencia desleal?

Cuestiones

1.- Certificados de atributos

2.- Certificados de pj

3.- E-DNI

III.No repudio y acuse de recibo

Ley 24/2001: nuevo art. 59.3 Ley 30/1992:

*“Para que la **notificación se practique utilizando medios telemáticos** se requerirá que el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización, identificando además la **dirección electrónica correspondiente**, que deberá cumplir con los requisitos reglamentariamente establecidos....”.*

III.No repudio y acuse de recibo

Ley 24/2001: nuevo art. 59.3 Ley 30/1992:

*“Para que la **notificación se practique utilizando medios telemáticos** se requerirá que el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización, identificando además la **dirección electrónica correspondiente, que deberá cumplir con los requisitos reglamentariamente establecidos**. En estos casos, la notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el **acceso a su contenido** en la dirección electrónica ...”.*

III. No repudio y acuse de recibo

Ley 24/2001: nuevo art. 59.3 Ley 30/1992:

*“Para que la **notificación se practique utilizando medios telemáticos** se requerirá que el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización, identificando además la **dirección electrónica correspondiente, que deberá cumplir con los requisitos reglamentariamente establecidos**. En estos casos, la notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el **acceso a su contenido** en la dirección electrónica. Cuando, existiendo constancia de la recepción de la notificación en la dirección electrónica, transcurrieran **diez días naturales sin que se acceda a su contenido**, se entenderá que **la notificación ha sido rechazada** con los efectos previstos en el siguiente apartado, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso”.*

IV. Reflexiones sobre el futuro de la firma electrónica en la e-A (A-E)

-Firma electrónica: aplicación real; perspectiva de futuro

-E-administración:

- Evolución del concepto y del contenido

- Necesidad de conjugar eficacia y seguridad

- Firma electrónica como instrumento de seguridad
(no único/idea de proporcionalidad)

- Especial aplicabilidad e idoneidad en el ámbito de la empresa:

 - Ejemplos pasados y presentes: AEAT, Seg.Social, Notarios, Registradores

 - Ejemplo futuro: Proyecto Sociedad Nueva Empresa

III. No repudio y acuse de recibo

Ley 24/2001: nuevo art. 59.3 Ley 30/1992:

*“Para que la **notificación se practique utilizando medios telemáticos** se requerirá que el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización, identificando además la **dirección electrónica correspondiente, que deberá cumplir con los requisitos reglamentariamente establecidos**. En estos casos, la notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el **acceso a su contenido** en la dirección electrónica. Cuando, existiendo constancia de la recepción de la notificación en la dirección electrónica, transcurrieran **diez días naturales sin que se acceda a su contenido**, se entenderá que **la notificación ha sido rechazada** con los efectos previstos en el siguiente apartado, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso”.*