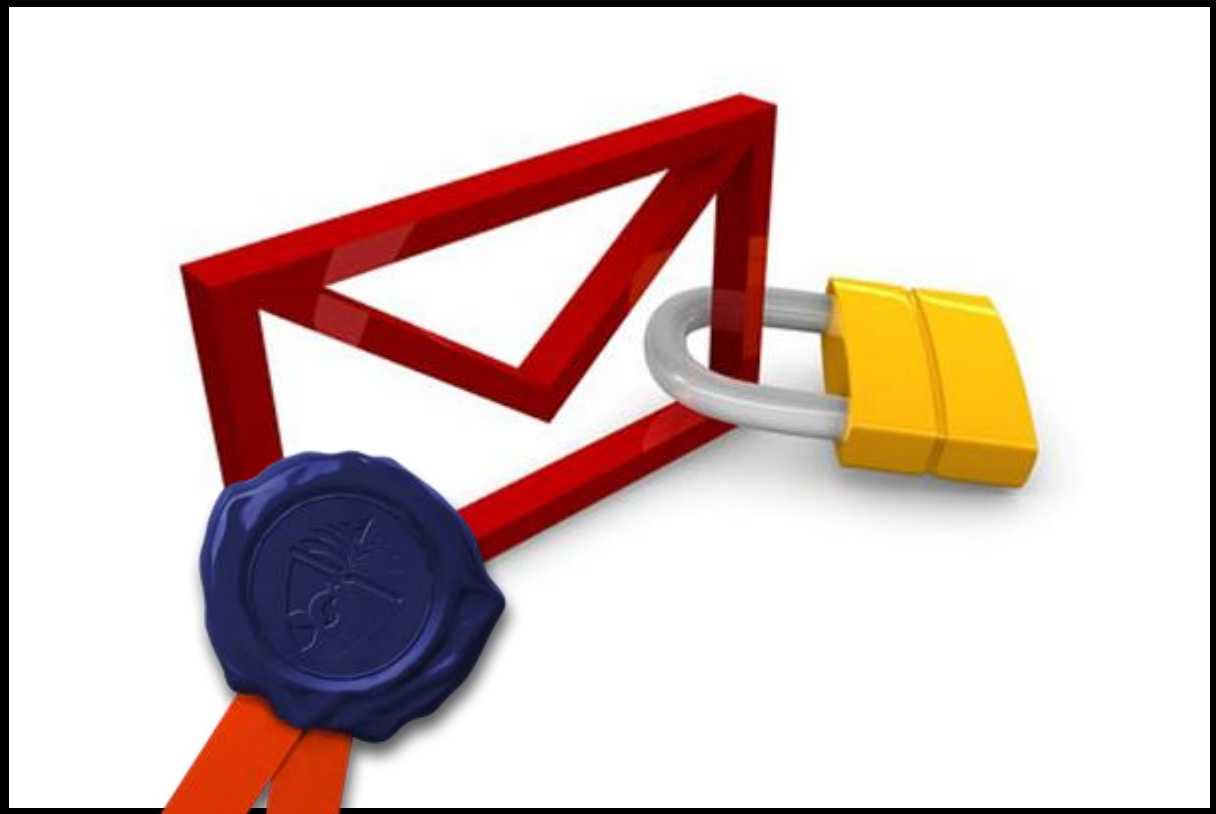
S/MIME



Miguel Macías Enguídanos

De: Foro T écnico de la Comunidad RedIRIS
En nombre de **Jesus Sanz de las Heras**
Enviado el: miércoles, 21 de mayo de 2014 16:40
Para: TECNIRIS@LISTSERV.REDIRIS.ES
Asunto: [TECNIRIS] Firmado y cifrado de correo

Buenas,

A veces nos quejamos de la falta dee confidencialidad de los datos almacenados, en nuestras comunicaciones.
Por el contrario creo que es minoritario el uso del correo cifrado (o firmado). Es una tema antiguo y siempre pendiente, pero la evolución tecnológica esta facilitando el uso de estas funcionalidades, que siguen sin utilizarse de forma amplia

Actualmente hay dos estándares (S/MIME, PGP) a la hora de cifrar / firmar digitalmente correos electrónicos. Tanto el uno como el otro tienen sus puntos fuertes y débiles. Ambos sistemas ofrecen tanto firmado digital (autenticidad, integridad de los datos) como cifrado de comunicaciones. GPG/PGP ha tenido una mayor difusión en internet y es el mas usado ... dentro de la poca gente que usa firmado/cifrado de correo. S/MIME siempre ha sido menos utilizado a pesar de venir 'de serie' en casi todos los clientes de correo.

El correo mantiene unos estándares y dentro de ellos se puede usar cualquier tipo de cliente (Web o IMAP). Lo mismo on el firmado/cifrado podemos utilizar GPG o S/MIME. Desde mi punto de vista S/MIME se ajustaría mejor a una estructura organizativa como la de RedIRIS. PGP se ajusta mas a una estructura mas individual . Los clientes de correo (Webmail e IMAP) facilitan el uso de S/MIME uso de forma sencilla y es una pena no aprovecharlo.
Ademas existen decenas de servidores de certificados FNMT, RedIRIS/TERNEA, Comodo etc fáciles de solicitar y revocar en caso de perdida.

Mi propuesta sería definir un plan para fomentar y facilitar el uso de cifrado y firmado para correos electrónicos en nuestros usuarios.
¿Merecería la pena?

SALUDos

El duque em...Palma...do: Iñaki Urdangarin bromeaba con su firma en correos al secretario de las infantas

EL EQUIPO CICLONUDISTA DE 'TXIKITIN'

Entre los correos electrónicos hay uno en el que se pone de manifiesto la estrecha relación que mantenían el duque de Palma y el secretario de las infantas. Bajo el asunto **'Me piro, cambio de curro'**, Iñaki Urdangarin explica a Carlos García Revenga que "aunque os va a sonar muy extraño, en estos momentos, os anuncio mi cambio de trabajo".

Un mail en tono jocoso, en donde el duque de Palma afirma que ha recibido una "excelente propuesta" para fichar por un equipo ciclista, iniciativa a la que ha

"Estoy 'sementaleando' tu propuesta". El inglés en los correos de Urdangarín

Piden tres años de cárcel para Miguel Blesa, que negó bajo juramento una relación sexual con una empleada. Sus correos descubren la verdad.

Los correos de Blesa a su amante de CajaMadrid

Así celebró Miguel Blesa el 'éxito' de las preferentes de Caja Madrid

De: Miguel Blesa de la Parra
Asunto: Re: Preferentes
Fecha: 26 de mayo de 2009 21:09
Para: Matias Amat Roca [redacted]

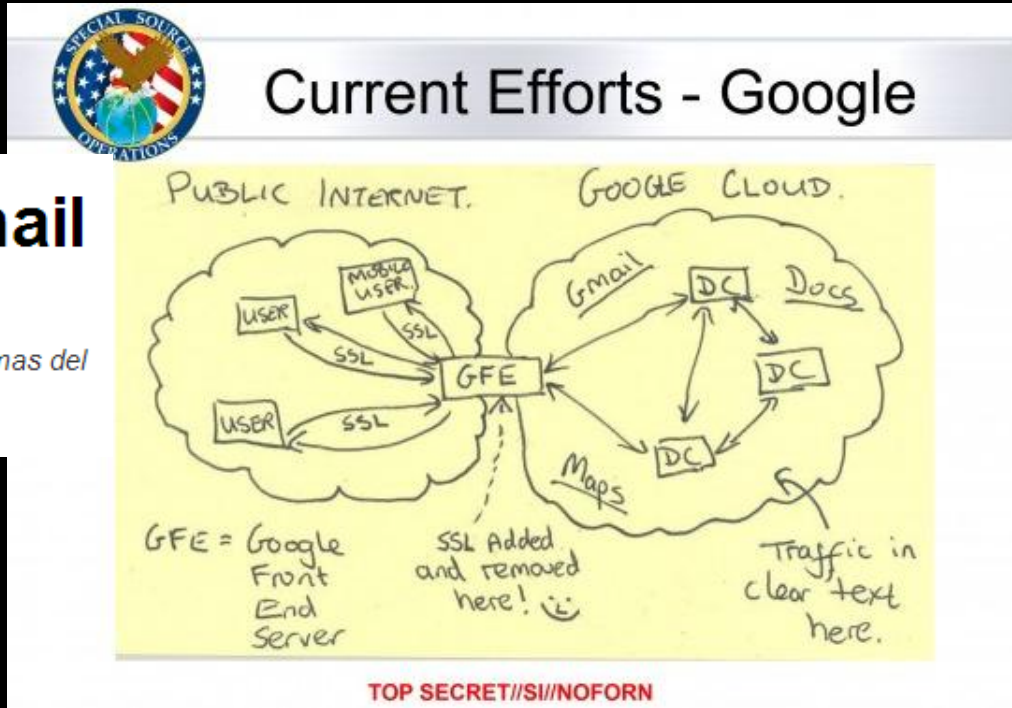
Que barbaro. Y eso que habiamops engaÑado a los clientes

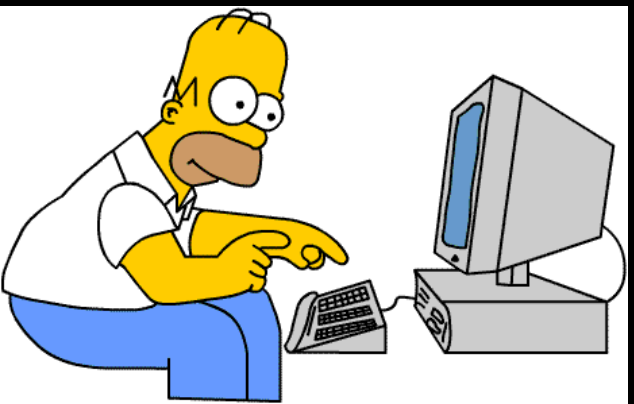
SEGURIDAD | Contenidos de e-mail o conversaciones de chat

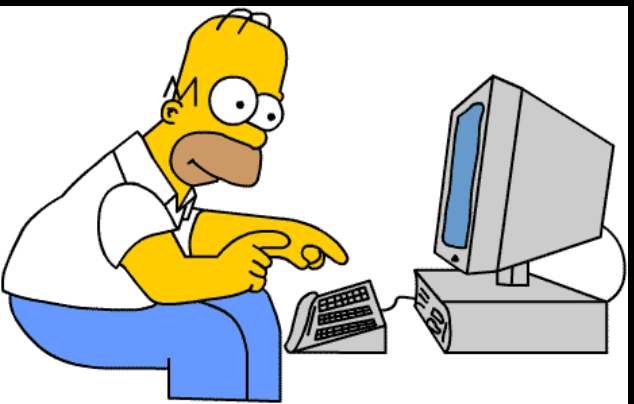
EEUU 'espía' a través de los servidores de Apple, Google o Facebook

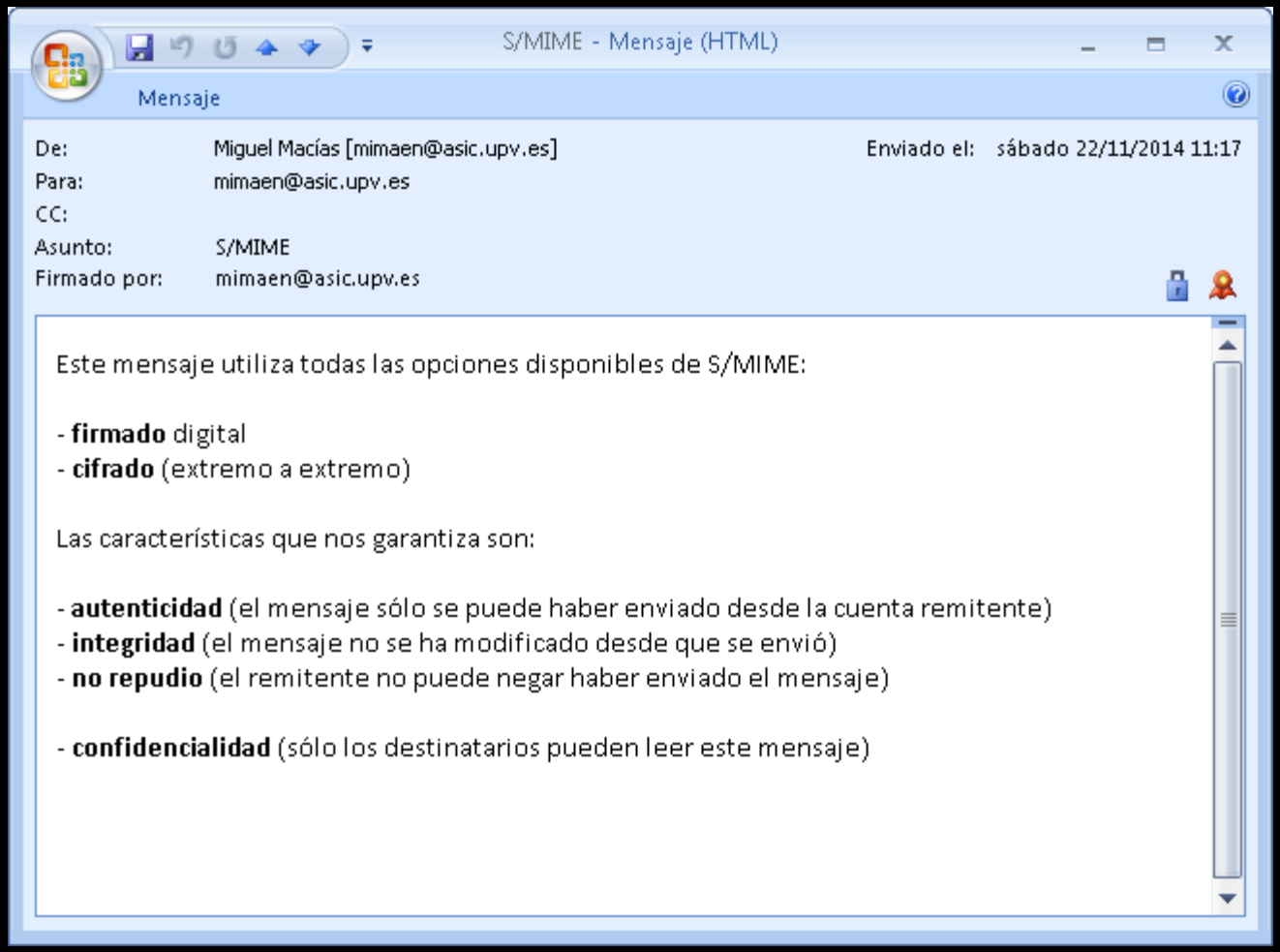
Así accede la NSA a tu Gmail

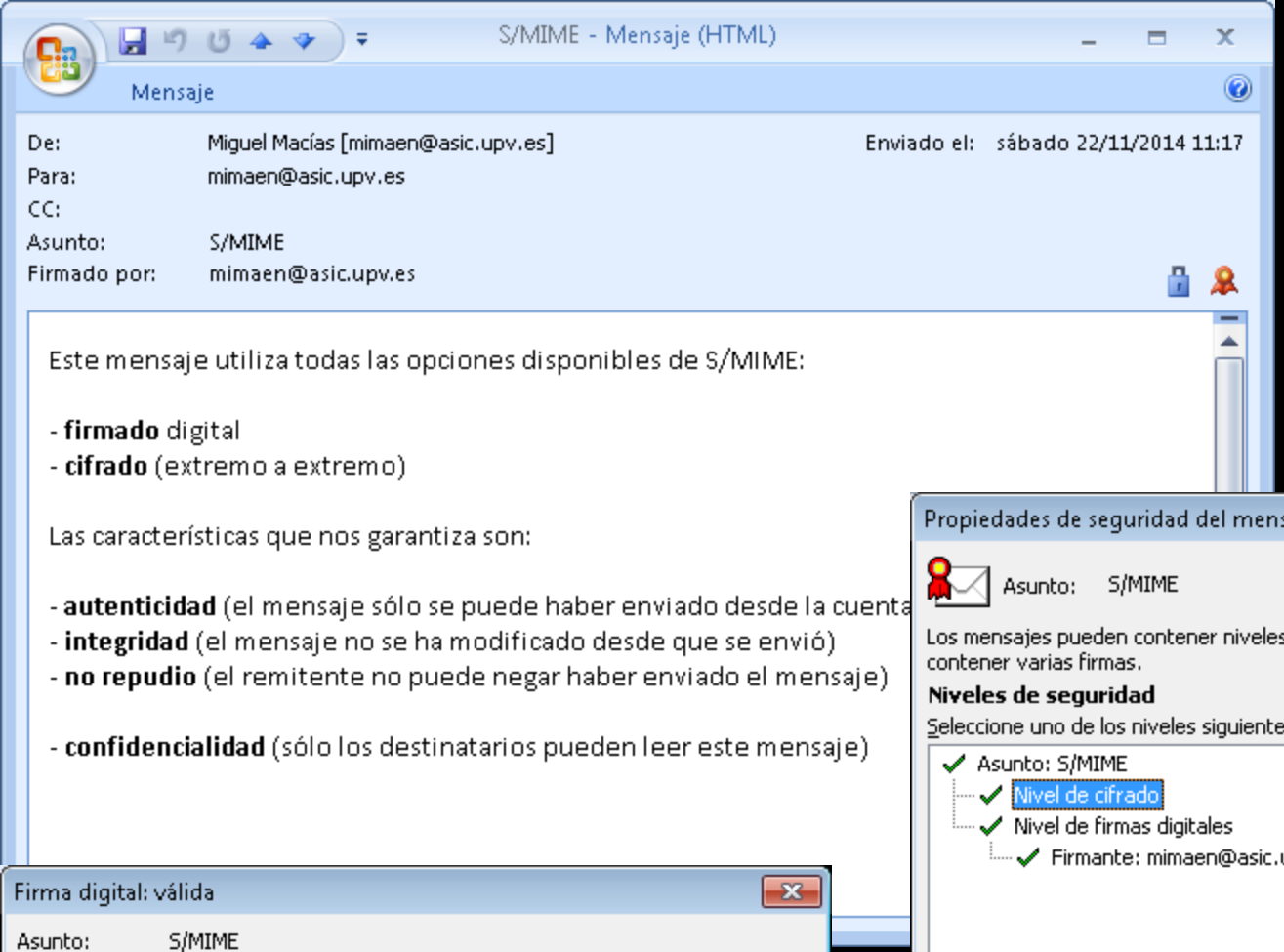
Intentamos explicar de manera sencilla cómo funcionan los 2 programas del Gobierno de EEUU que recogen nuestros datos en Internet.

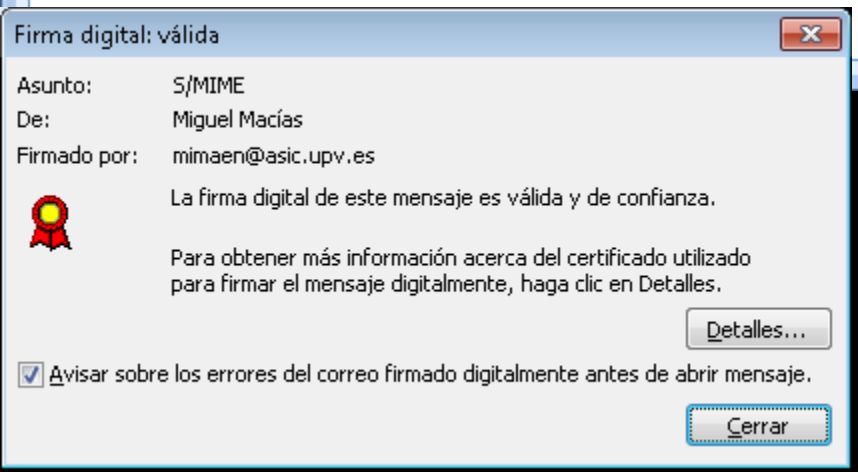


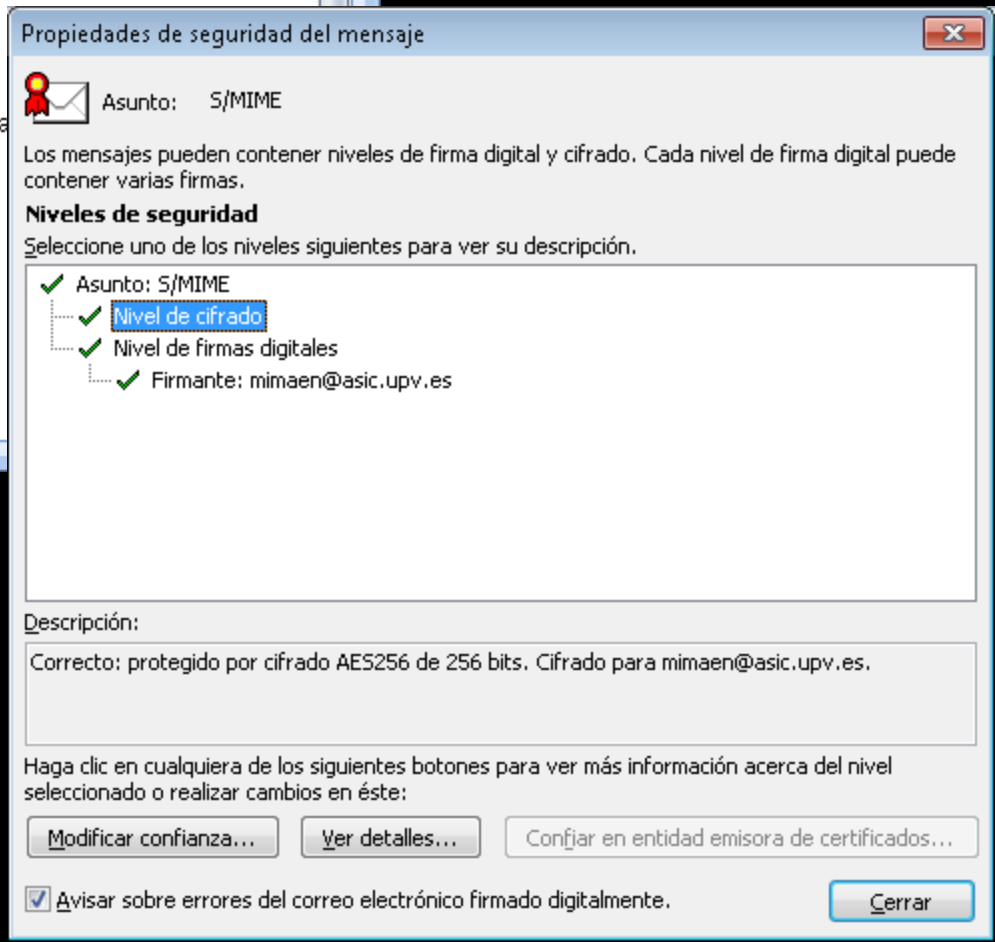





S/MIME - Mensaje (HTML)
Mensaje
De: Miguel Macías [mimaen@asic.upv.es]
Enviado el: sábado 22/11/2014 11:17
Para: mimaen@asic.upv.es
CC:
Asunto: S/MIME
Firmado por: mimaen@asic.upv.es
Este mensaje utiliza todas las opciones disponibles de S/MIME:
- firmado digital
- cifrado (extremo a extremo)
Las características que nos garantiza son:
- autenticidad (el mensaje sólo se puede haber enviado desde la cuenta remitente)
- integridad (el mensaje no se ha modificado desde que se envió)
- no repudio (el remitente no puede negar haber enviado el mensaje)
- confidencialidad (sólo los destinatarios pueden leer este mensaje)


S/MIME - Mensaje (HTML)
Mensaje
De: Miguel Macías [mimaen@asic.upv.es]
Enviado el: sábado 22/11/2014 11:17
Para: mimaen@asic.upv.es
CC:
Asunto: S/MIME
Firmado por: mimaen@asic.upv.es
Este mensaje utiliza todas las opciones disponibles de S/MIME:
- firmado digital
- cifrado (extremo a extremo)
Las características que nos garantiza son:
- autenticidad (el mensaje sólo se puede haber enviado desde la cuenta
- integridad (el mensaje no se ha modificado desde que se envió)
- no repudio (el remitente no puede negar haber enviado el mensaje)
- confidencialidad (sólo los destinatarios pueden leer este mensaje)


Firma digital: válida
Asunto: S/MIME
De: Miguel Macías
Firmado por: mimaen@asic.upv.es
La firma digital de este mensaje es válida y de confianza.
Para obtener más información acerca del certificado utilizado para firmar el mensaje digitalmente, haga clic en Detalles.
Detalles...
Avisar sobre los errores del correo firmado digitalmente antes de abrir mensaje.
Cerrar


Propiedades de seguridad del mensaje
Asunto: S/MIME
Los mensajes pueden contener niveles de firma digital y cifrado. Cada nivel de firma digital puede contener varias firmas.
Niveles de seguridad
Seleccione uno de los niveles siguientes para ver su descripción.
Asunto: S/MIME
Nivel de cifrado
Nivel de firmas digitales
Firmante: mimaen@asic.upv.es
Descripción:
Correcto: protegido por cifrado AES256 de 256 bits. Cifrado para mimaen@asic.upv.es.
Haga clic en cualquiera de los siguientes botones para ver más información acerca del nivel seleccionado o realizar cambios en éste:
Modificar confianza...
Ver detalles...
Confiar en entidad emisora de certificados...
Avisar sobre errores del correo electrónico firmado digitalmente.
Cerrar

De Miguel Macías <mimaen@asic.upv.es>

Asunto **S/MIME**

A mimaen@asic.upv.es

22/11/2014 11:17

Otras acciones

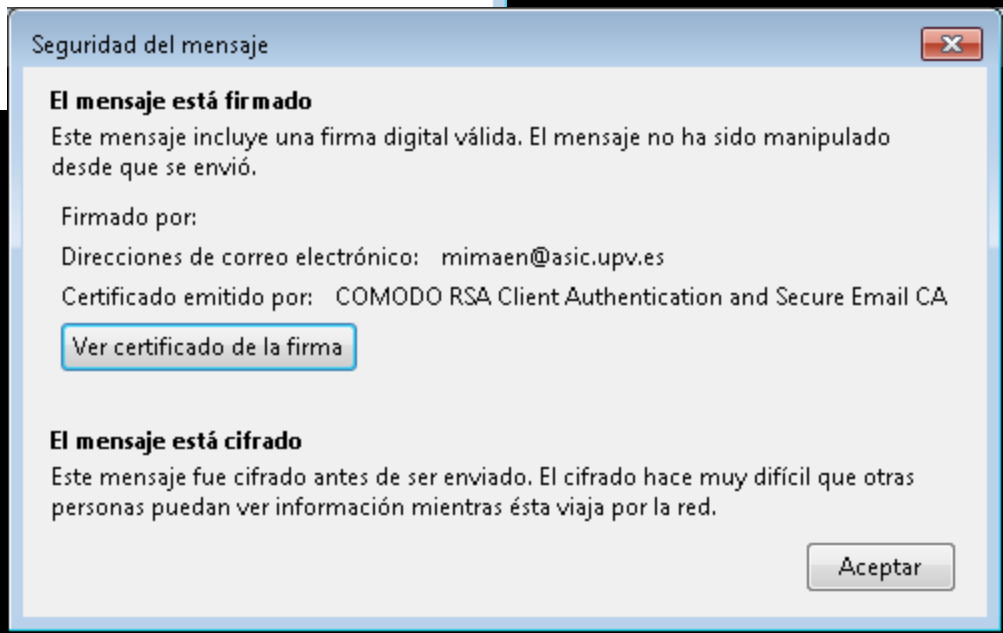
Este mensaje utiliza todas las opciones disponibles de S/MIME:

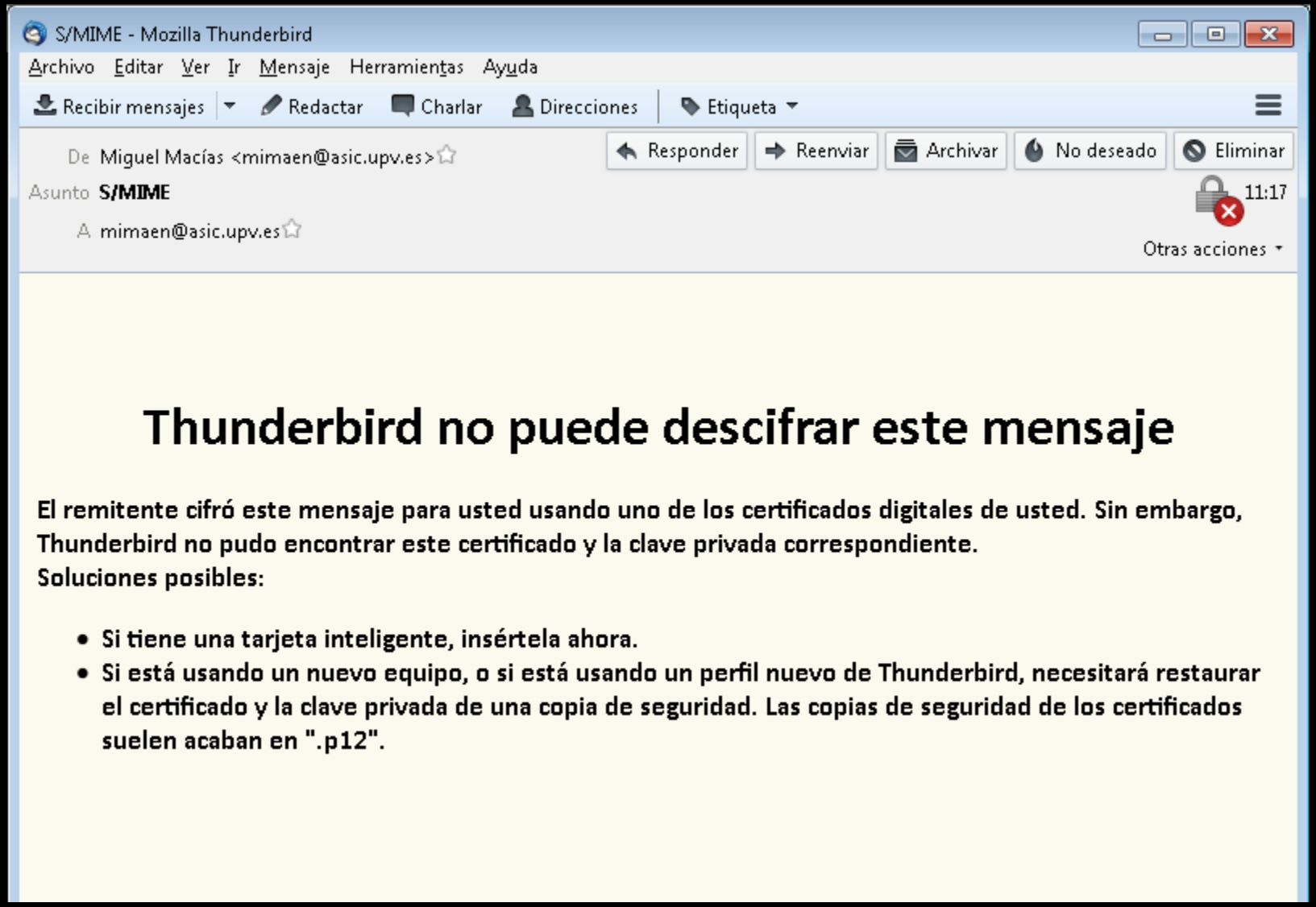
- **firmado** digital
- **cifrado** (extremo a extremo)

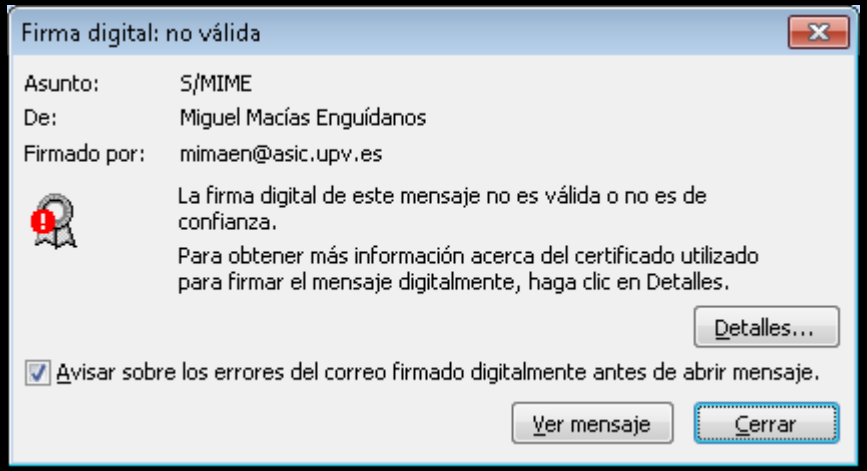
Las características que nos garantiza son:

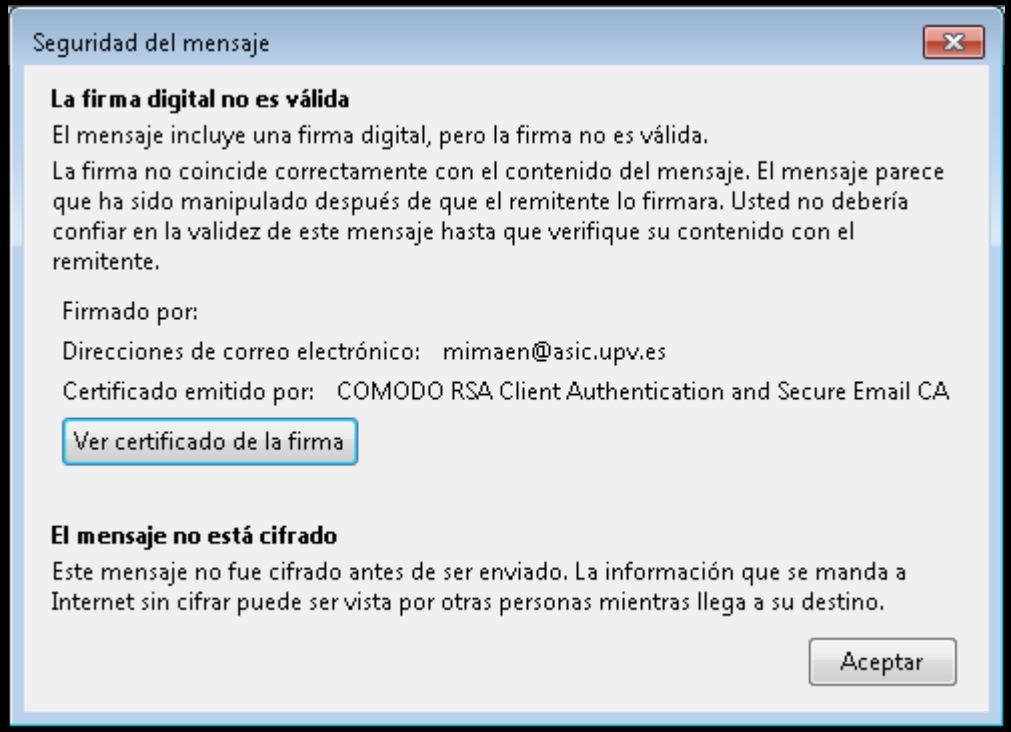
- **autenticidad** (el mensaje sólo se puede haber enviado desde la cuenta remitente)
- **integridad** (el mensaje no se ha modificado desde que se envió)
- **no repudio** (el remitente no puede negar haber enviado el mensaje)

- **confidencialidad** (sólo los destinatarios pueden leer este mensaje)




S/MIME - Mozilla Thunderbird
Archivo Editar Ver Ir Mensaje Herramientas Ayuda
Recibir mensajes
Redactar
Charlar
Direcciones
Etiqueta
De Miguel Macías <mimaen@asic.upv.es>
Asunto S/MIME
A mimaen@asic.upv.es
Responder
Reenviar
Archivar
No deseado
Eliminar
11:17
Otras acciones
Thunderbird no puede descifrar este mensaje
El remitente cifró este mensaje para usted usando uno de los certificados digitales de usted. Sin embargo, Thunderbird no pudo encontrar este certificado y la clave privada correspondiente.
Soluciones posibles:
Si tiene una tarjeta inteligente, insértela ahora.
Si está usando un nuevo equipo, o si está usando un perfil nuevo de Thunderbird, necesitará restaurar el certificado y la clave privada de una copia de seguridad. Las copias de seguridad de los certificados suelen acaban en ".p12".


Firma digital: no válida
Asunto: S/MIME
De: Miguel Macías Enguídanos
Firmado por: mimaen@asic.upv.es
La firma digital de este mensaje no es válida o no es de confianza.
Para obtener más información acerca del certificado utilizado para firmar el mensaje digitalmente, haga clic en Detalles.
Detalles...
Avisar sobre los errores del correo firmado digitalmente antes de abrir mensaje.
Ver mensaje
Cerrar


Seguridad del mensaje
La firma digital no es válida
El mensaje incluye una firma digital, pero la firma no es válida.
La firma no coincide correctamente con el contenido del mensaje. El mensaje parece que ha sido manipulado después de que el remitente lo firmara. Usted no debería confiar en la validez de este mensaje hasta que verifique su contenido con el remitente.
Firmado por:
Direcciones de correo electrónico: mimaen@asic.upv.es
Certificado emitido por: COMODO RSA Client Authentication and Secure Email CA
Ver certificado de la firma
El mensaje no está cifrado
Este mensaje no fue cifrado antes de ser enviado. La información que se manda a Internet sin cifrar puede ser vista por otras personas mientras llega a su destino.
Aceptar

http://www.rediris.es/scs/perfil/personal/

https://www.instantssl.com/

COMODO
Creating Trust Online®

FREE

https://www.startssl.com/

StartSSL™ PKI


DOH!

1

De Jesus Sanz de las Heras <jesus.heras@rediris.es>

Asunto **[TECNIRIS] Firmado y cifrado de correo**

A TECNIRIS@LISTSERV.REDIRIS.ES

21/05/2014 16:39

Otras acciones

Buenas,

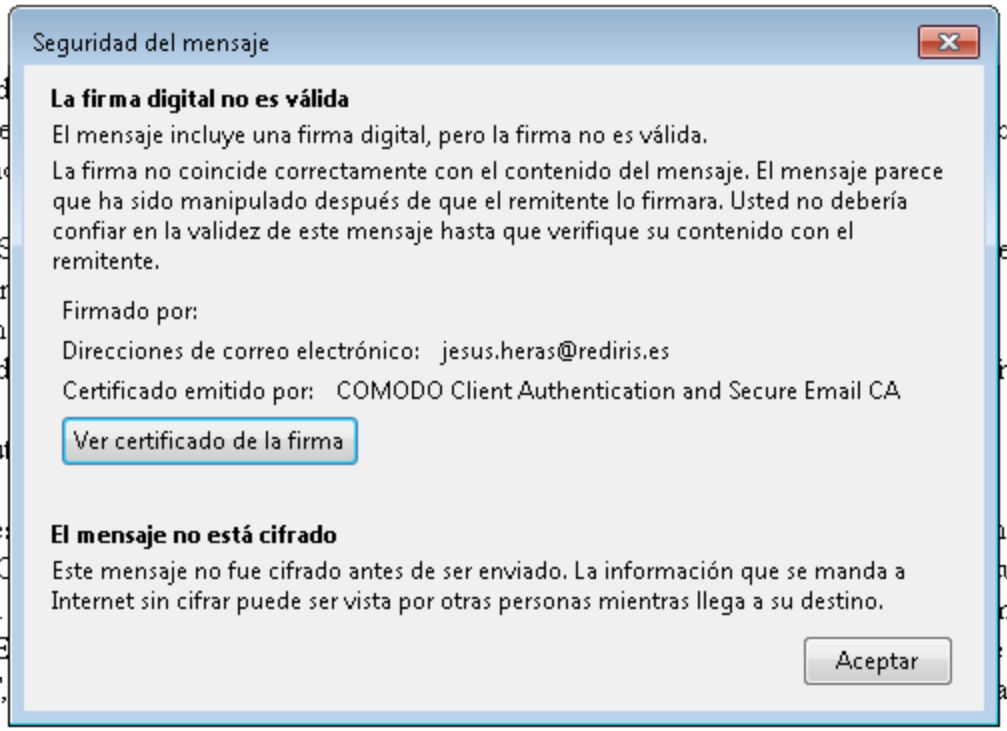
A veces nos quejamos de la falta d
contrario creo que es minoritario e
evolución tecnológica esta facilitan

Actualmente hay dos estándares (S
como el otro tienen sus puntos fuer
Ambos sistemas ofrecen tanto firm
GPG/PGP ha tenido una mayor d
correo.
S/MIME siempre ha sido menos ut

El correo mantiene unos estándare
firmado/cifrado podemos utilizar C
organizativa como la de RedIRIS.
IMAP) facilitan el uso de S/MIME
servidores de certificados FNMT,

Mi propuesta sería definir un plan para fomentar y facilitar el uso de cifrado y firmado para correos electrónicos en nuestros usuarios.
¿Merecería la pena?

SALUDos
--
Jesús Sanz de las Heras



```
MIME-Version: 1.0
Content-Type: multipart/signed;
              protocol="application/pkcs7-signature";
              micalg=sha1;
              boundary="----=_Part_1196_539502381.1400683170646”
```

```
------=_Part_1196_539502381.1400683170646
Content-Type: multipart/alternative;
       boundary="----=_Part_1194_1143732196.1400683170587"
```

```
------=_Part_1194_1143732196.1400683170587
Content-Type: text/plain; charset=UTF-8
…
SALUDos=20
--=20
…
-------------------------------------------------
Consigue certificados gratuitos para servidores con SCS
+info: http://www.rediris.es/scs
-------------------------------------------------
```

```
MIME-Version: 1.0
Content-Type: multipart/signed;
              protocol="application/pkcs7-signature";
              micalg=sha1;
              boundary="----=_Part_1196_539502381.1400683170646”
```

```
------=_Part_1196_539502381.1400683170646
Content-Type: multipart/alternative;
       boundary="----=_Part_1194_1143732196.1400683170587"
```

```
------=_Part_1194_1143732196.1400683170587
Content-Type: text/html; charset=UTF-8
…
iv style=3D"text-align: justify">SALUDos<br><span
style=3D"font-family: com=
…
<p align=3D"left">=C2=BFConoce el <a
href=3D"http://www.rediris.es/tecniris/programa/">Programa
de videoSesiones TECNIRIS@?</a><br>
```

```
MIME-Version: 1.0
Content-Type: multipart/signed;
              protocol="application/pkcs7-signature";
              micalg=sha1;
              boundary="----=_Part_1196_539502381.1400683170646”
```

```
------=_Part_1196_539502381.1400683170646
Content-Type: multipart/alternative;
       boundary="----=_Part_1194_1143732196.1400683170587"
```

```
------=_Part_1196_539502381.1400683170646
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQ
AAoIIO9jCCBKIw
```

De Jesus Sanz de las Heras <jesus.heras@rediris.es>

Asunto **[TECNIRIS] Firmado y cifrado de correo**

21/05/2014 16:39

A TECNIRIS@LISTSERV.REDIRIS.ES

Otras acciones

firmado/cifrado podemos utilizar GPG o S/MIME. Desde mi punto de vista S/MIME se ajustaría mejor a una estructura organizativa como la de RedIRIS. PGP se ajusta mas a una estructura mas individual . Los clientes de correo (Webmail e IMAP) facilitan el uso de S/MIME uso de forma sencilla y es una pena no aprovecharlo. Ademas existen decenas de servidores de certificados FNMT, RedIRIS/TERNEA, Comodo etc fáciles de solicitar y revocar en caso de perdida.

Mi propuesta sería definir un plan para fomentar y facilitar el uso de cifrado y firmado para correos electrónicos en nuestros usuarios.
¿Merecería la pena?

SALUDos
--
Jesús Sanz de las Heras
RedIRIS /red.es
Email Systems security & abuse
LISTSERV manager
Tel: 675.544.214
- Spain's Academic & Research Network (www.rediris.es) -

De Jesus Sanz de las Heras <jesus.heras@rediris.es>

Asunto **[TECNIRIS] Firmado y cifrado de correo**

21/05/2014 16:39

A TECNIRIS@LISTSERV.REDIRIS.ES

Otras acciones

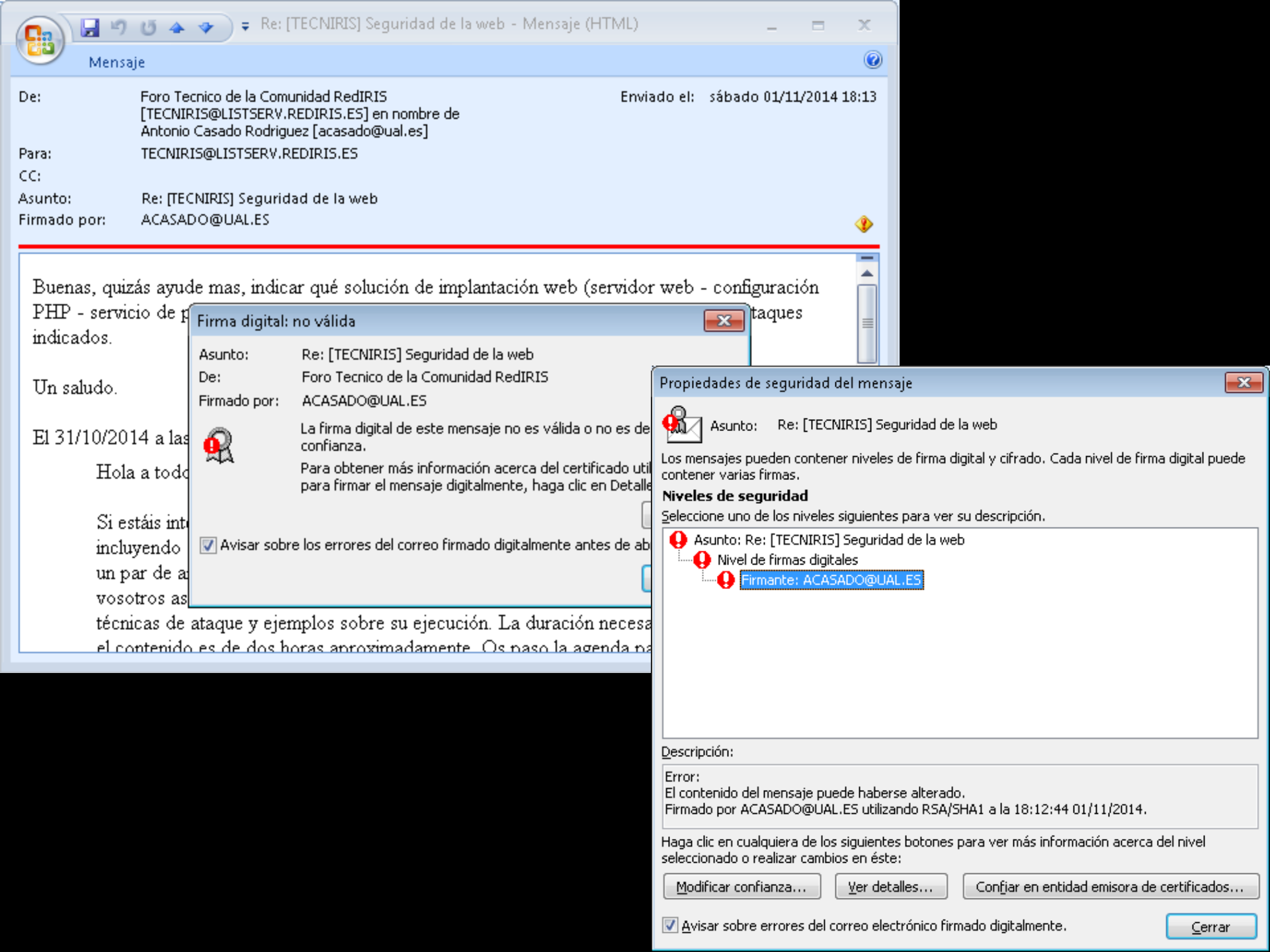
firmado/cifrado podemos utilizar GPG o S/MIME. Desde mi punto de vista S/MIME se ajustaría mejor a una estructura organizativa como la de RedIRIS. PGP se ajusta mas a una estructura mas individual . Los clientes de correo (Webmail e IMAP) facilitan el uso de S/MIME uso de forma sencilla y es una pena no aprovecharlo. Ademas existen decenas de servidores de certificados FNMT, RedIRIS/TERNEA, Comodo etc fáciles de solicitar y revocar en caso de perdida.

Mi propuesta sería definir un plan para fomentar y facilitar el uso de cifrado y firmado para correos electrónicos en nuestros usuarios.
¿Merecería la pena?

SALUDos

--
Jesús Sanz de las Heras
RedIRIS /red.es
Email Systems security & abuse
LISTSERV manager
Tel: 675.544.214
- Spain's Academic & Research Network (www.rediris.es) -

¿Conoce el Programa de videoSesiones TECNIRIS@?


Re: [TECNIRIS] Seguridad de la web - Mensaje (HTML)
Mensaje
De: Foro Tecnico de la Comunidad RedIRIS [TECNIRIS@LISTSERV.REDIRIS.ES] en nombre de Antonio Casado Rodriguez [acasado@ual.es]
Enviado el: sábado 01/11/2014 18:13
Para: TECNIRIS@LISTSERV.REDIRIS.ES
CC:
Asunto: Re: [TECNIRIS] Seguridad de la web
Firmado por: ACASADO@UAL.ES
Buenas, quizás ayude mas, indicar qué solución de implantación web (servidor web - configuración PHP - servicio de p
taques
indicados.
Un saludo.
El 31/10/2014 a las
Hola a todo
Si estáis int
incluyendo
un par de a
vosotros as
técnicas de ataque y ejemplos sobre su ejecución. La duración necesa
el contenido es de dos horas aproximadamente. Os paso la agenda pa
Firma digital: no válida
Asunto: Re: [TECNIRIS] Seguridad de la web
De: Foro Tecnico de la Comunidad RedIRIS
Firmado por: ACASADO@UAL.ES
La firma digital de este mensaje no es válida o no es de
confianza.
Para obtener más información acerca del certificado util
para firmar el mensaje digitalmente, haga clic en Detalle
Avisar sobre los errores del correo firmado digitalmente antes de ab
Propiedades de seguridad del mensaje
Asunto: Re: [TECNIRIS] Seguridad de la web
Los mensajes pueden contener niveles de firma digital y cifrado. Cada nivel de firma digital puede contener varias firmas.
Niveles de seguridad
Seleccione uno de los niveles siguientes para ver su descripción.
Asunto: Re: [TECNIRIS] Seguridad de la web
Nivel de firmas digitales
Firmante: ACASADO@UAL.ES
Descripción:
Error:
El contenido del mensaje puede haberse alterado.
Firmado por ACASADO@UAL.ES utilizando RSA/SHA1 a la 18:12:44 01/11/2014.
Haga clic en cualquiera de los siguientes botones para ver más información acerca del nivel seleccionado o realizar cambios en éste:
Modificar confianza...
Ver detalles...
Confiar en entidad emisora de certificados...
Avisar sobre errores del correo electrónico firmado digitalmente.
Cerrar

Re: [TECNIRIS] Limpieza de metadatos - Mensaje (HTML)

Mensaje

De: Foro Tecnico de la Comunidad RedIRIS [TECNIRIS@LISTSERV.REDIRIS.ES] en nombre de Antonio Casado Rodriguez [acasado@ual.es]

Enviado el: martes 04/11/2014 13:09

Para: TECNIRIS@LISTSERV.REDIRIS.ES

CC:

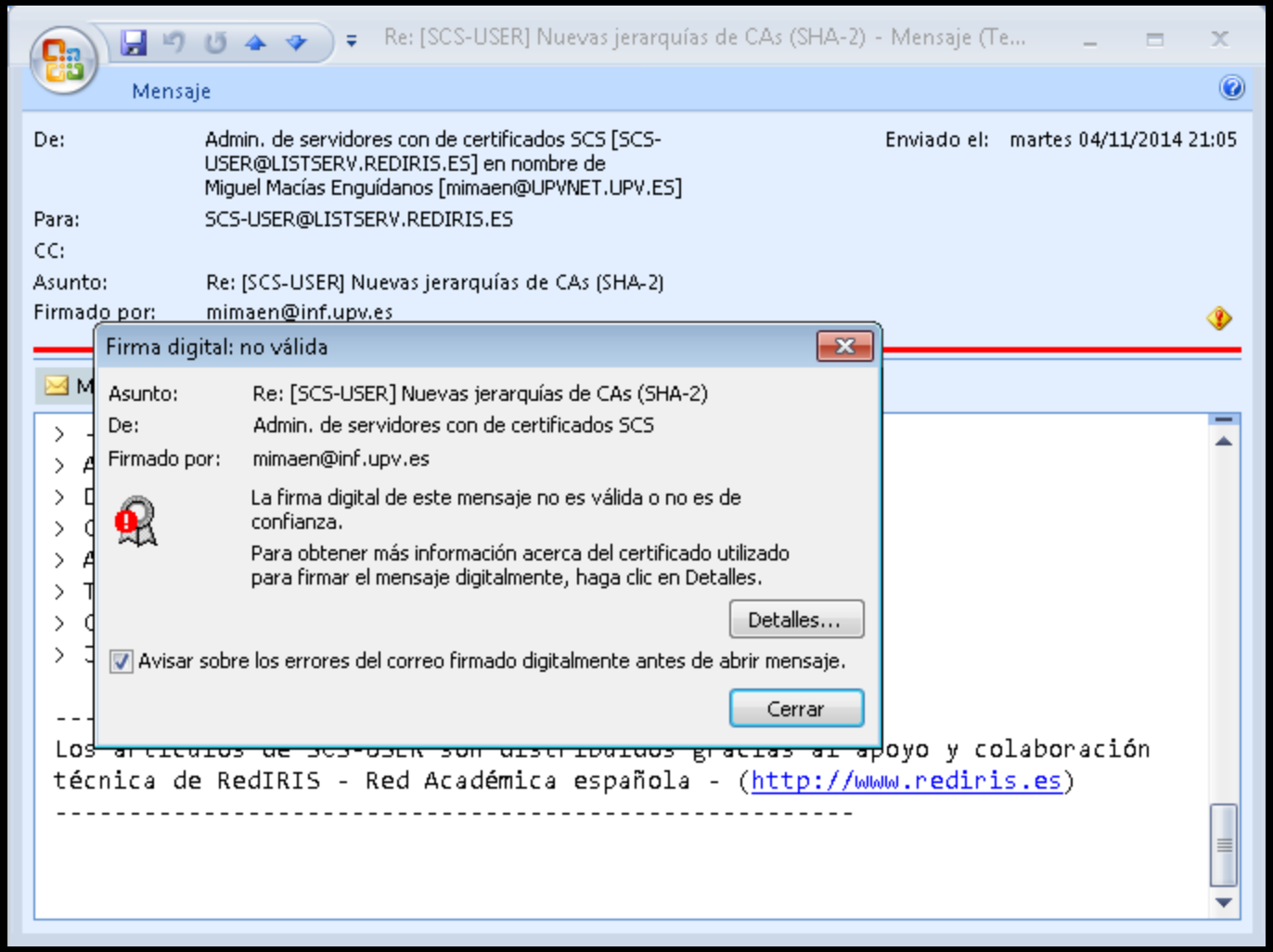
Asunto: Re: [TECNIRIS] Limpieza de metadatos

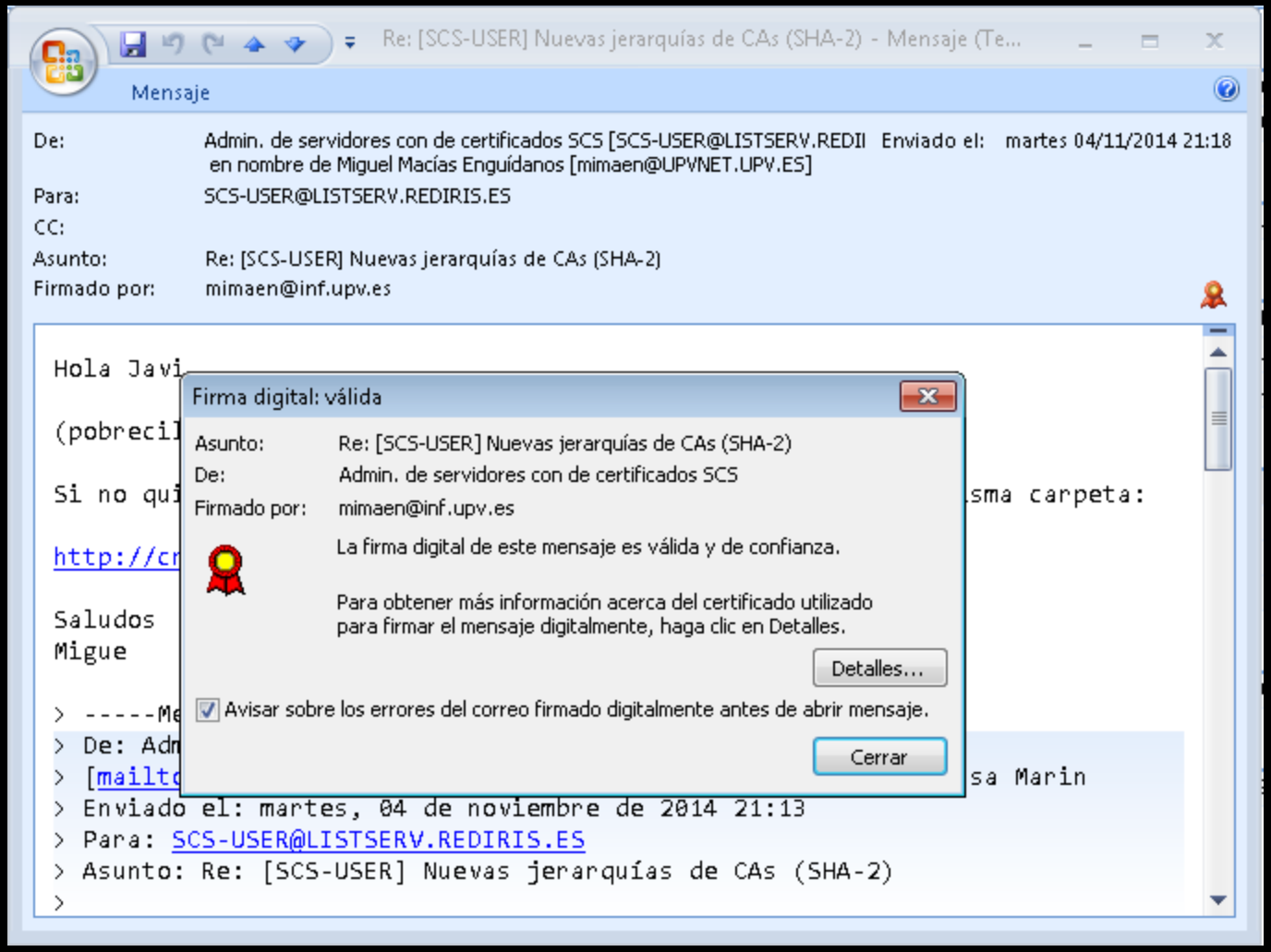
Muchas gracias a todos, veremos que podemos sacar en claro :-)

Saludos.

El 04/11/2014 a las 11:38, "SER.RI-TIC - Toni Cortès" escribió:

> Olvidé mencionar MAT Metadata Anonymisation Toolkit (imperdonable error para un linuxero :O) basado en python. Mediante GUI o CLI, puede limpiar o simplemente analizar y avisar de lo que llama "harmful metadata" :P
> https://mat.boum.org/
>
> Un saludo
>
> El 04/11/14 a les 11:22, "SER.RI-TIC - Toni Cortès" ha escrit:
>
> > Hola,

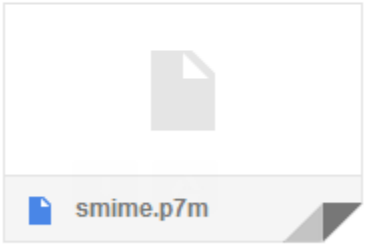

Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2) - Mensaje (Te...
Mensaje
De: Admin. de servidores con de certificados SCS [SCS-USER@LISTSERV.REDIRIS.ES] en nombre de Miguel Macías Enguídanos [mimaen@UPVNET.UPV.ES]
Enviado el: martes 04/11/2014 21:05
Para: SCS-USER@LISTSERV.REDIRIS.ES
CC:
Asunto: Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2)
Firmado por: mimaen@inf.upv.es
Firma digital: no válida
Asunto: Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2)
De: Admin. de servidores con de certificados SCS
Firmado por: mimaen@inf.upv.es
La firma digital de este mensaje no es válida o no es de confianza.
Para obtener más información acerca del certificado utilizado para firmar el mensaje digitalmente, haga clic en Detalles.
Detalles...
Avisar sobre los errores del correo firmado digitalmente antes de abrir mensaje.
Cerrar
técnica de RedIRIS - Red Académica española - (http://www.rediris.es)


Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2) - Mensaje (Te...
Mensaje
De: Admin. de servidores con de certificados SCS [SCS-USER@LISTSERV.REDII en nombre de Miguel Macías Enguídanos [mimaen@UPVNET.UPV.ES]
Enviado el: martes 04/11/2014 21:18
Para: SCS-USER@LISTSERV.REDIRIS.ES
CC:
Asunto: Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2)
Firmado por: mimaen@inf.upv.es
Hola Javi
(pobrecil
Si no qui
sma carpeta:
http://cr
Saludos
Migue
> -----Me
> De: Adm
> [mailto
sa Marin
> Enviado el: martes, 04 de noviembre de 2014 21:13
> Para: SCS-USER@LISTSERV.REDIRIS.ES
> Asunto: Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2)
>
Firma digital: válida
Asunto: Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2)
De: Admin. de servidores con de certificados SCS
Firmado por: mimaen@inf.upv.es
La firma digital de este mensaje es válida y de confianza.
Para obtener más información acerca del certificado utilizado para firmar el mensaje digitalmente, haga clic en Detalles.
Detalles...
Avisar sobre los errores del correo firmado digitalmente antes de abrir mensaje.
Cerrar

RE: [SCS-USER] Nuevas jerarquías de CAs (SHA-2) Recibidos x

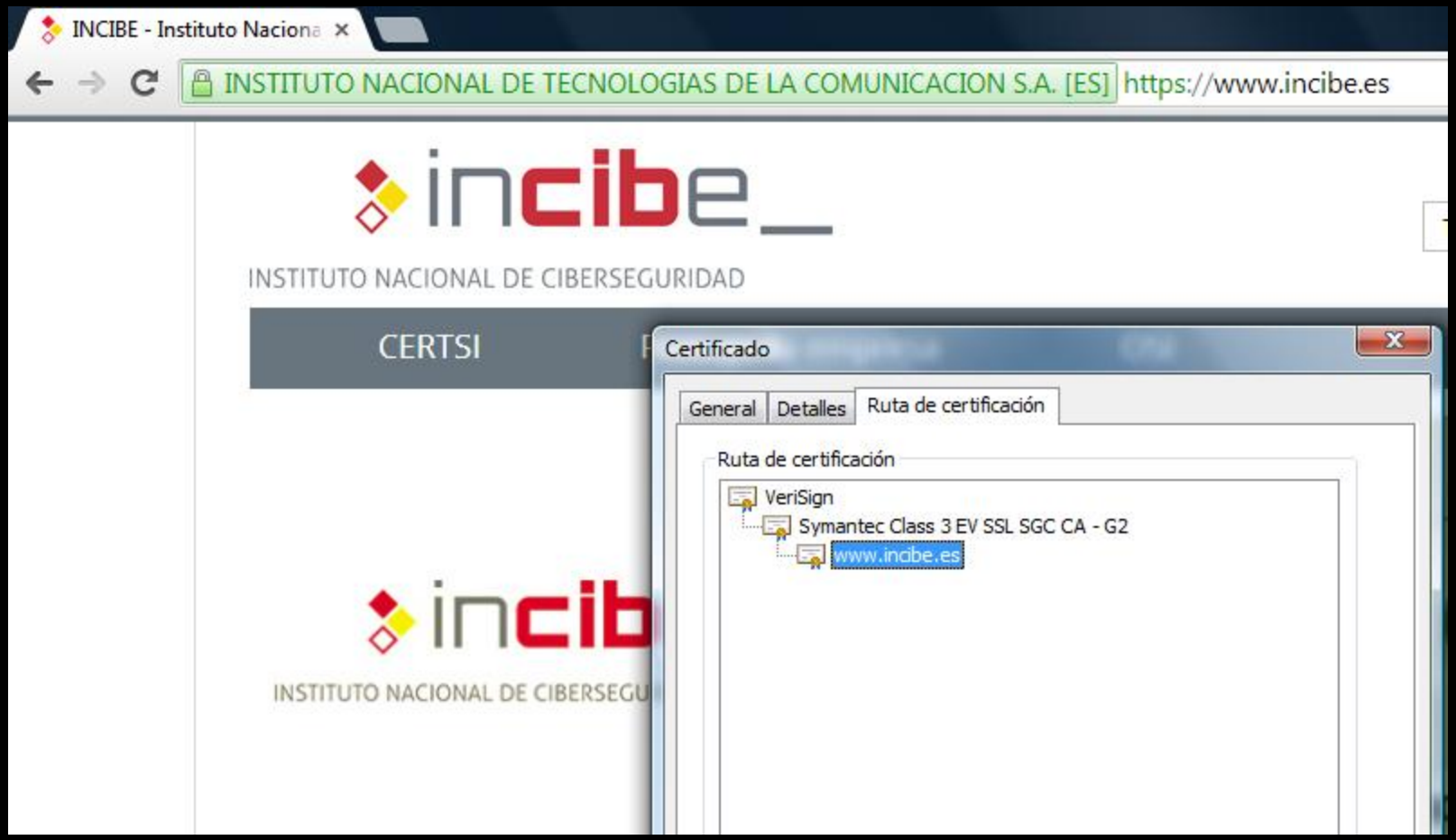
Miguel Macías Enguídanos 4 de nov.

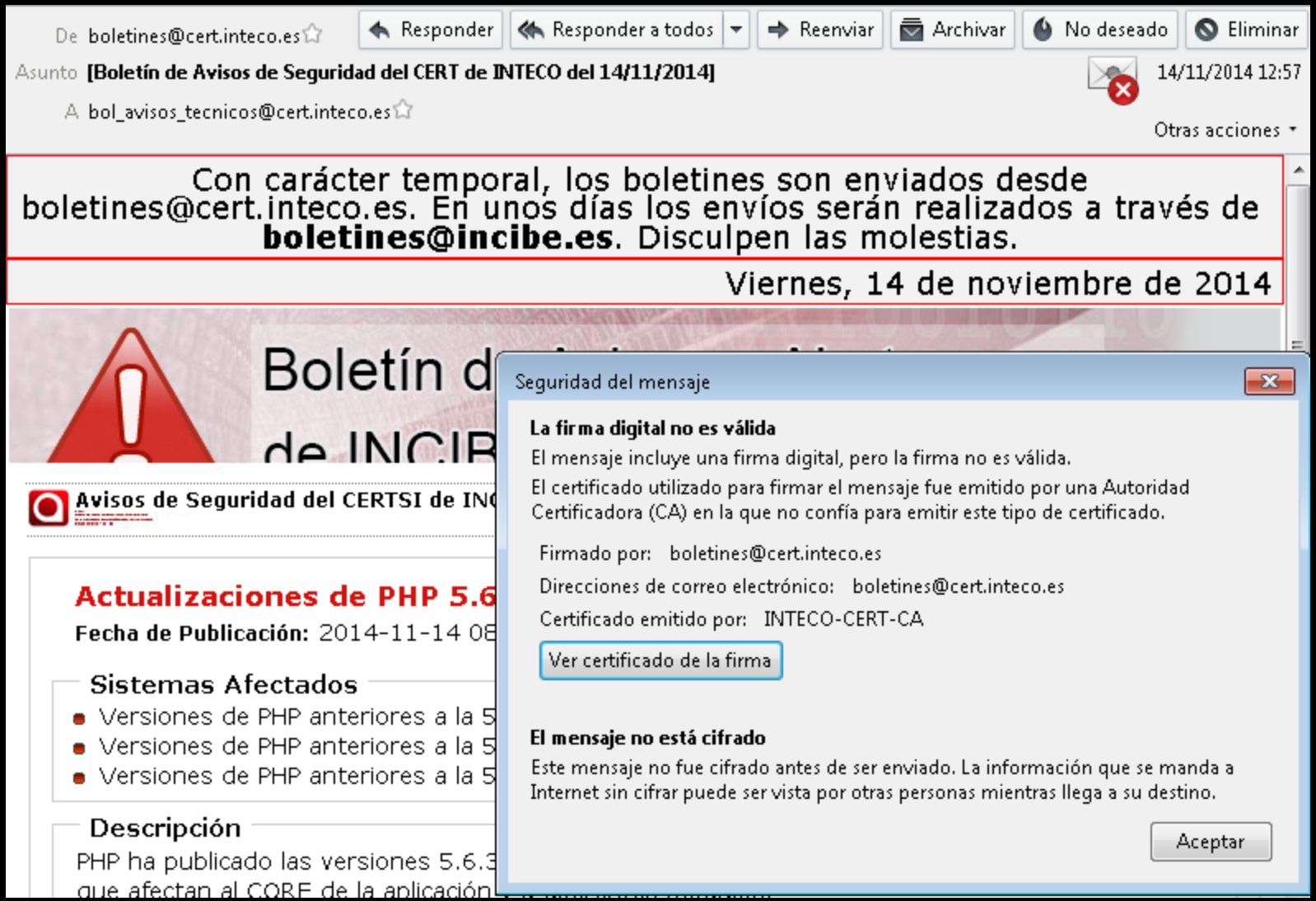
para de



smime.p7m

2


INCIBE - Instituto Nacional
INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACION S.A. [ES]
https://www.incibe.es
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
CERTSI
Certificado
General
Detalles
Ruta de certificación
Ruta de certificación
VeriSign
Symantec Class 3 EV SSL SGC CA - G2
www.incibe.es


De boletines@cert.inteco.es
Responder
Responder a todos
Reenviar
Archivar
No deseado
Eliminar
Asunto [Boletín de Avisos de Seguridad del CERT de INTECO del 14/11/2014]
14/11/2014 12:57
A bol_avisos_tecnicos@cert.inteco.es
Otras acciones
Con carácter temporal, los boletines son enviados desde boletines@cert.inteco.es. En unos días los envíos serán realizados a través de boletines@incibe.es. Disculpen las molestias.
Viernes, 14 de noviembre de 2014
Boletín d
de INCIB
Avisos de Seguridad del CERTSI de IN
Actualizaciones de PHP 5.6
Fecha de Publicación: 2014-11-14 08
Sistemas Afectados
Versiones de PHP anteriores a la 5
Versiones de PHP anteriores a la 5
Versiones de PHP anteriores a la 5
Descripción
PHP ha publicado las versiones 5.6.3
que afectan al CORE de la aplicación
Seguridad del mensaje
La firma digital no es válida
El mensaje incluye una firma digital, pero la firma no es válida.
El certificado utilizado para firmar el mensaje fue emitido por una Autoridad Certificadora (CA) en la que no confía para emitir este tipo de certificado.
Firmado por: boletines@cert.inteco.es
Direcciones de correo electrónico: boletines@cert.inteco.es
Certificado emitido por: INTECO-CERT-CA
Ver certificado de la firma
El mensaje no está cifrado
Este mensaje no fue cifrado antes de ser enviado. La información que se manda a Internet sin cifrar puede ser vista por otras personas mientras llega a su destino.
Aceptar

3

S/MIME - Mensaje (HTML)

Mensaje

De: Miguel Macías Enguídanos [mimaen@asic.upv.es]
Para: mimaen@asic.upv.es
CC:
Asunto: S/MIME
Firmado por: MIMAEN@ASIC.UPV.ES

Enviado el: sábado 22/11/2014 17:31

Este mensaje utiliza:

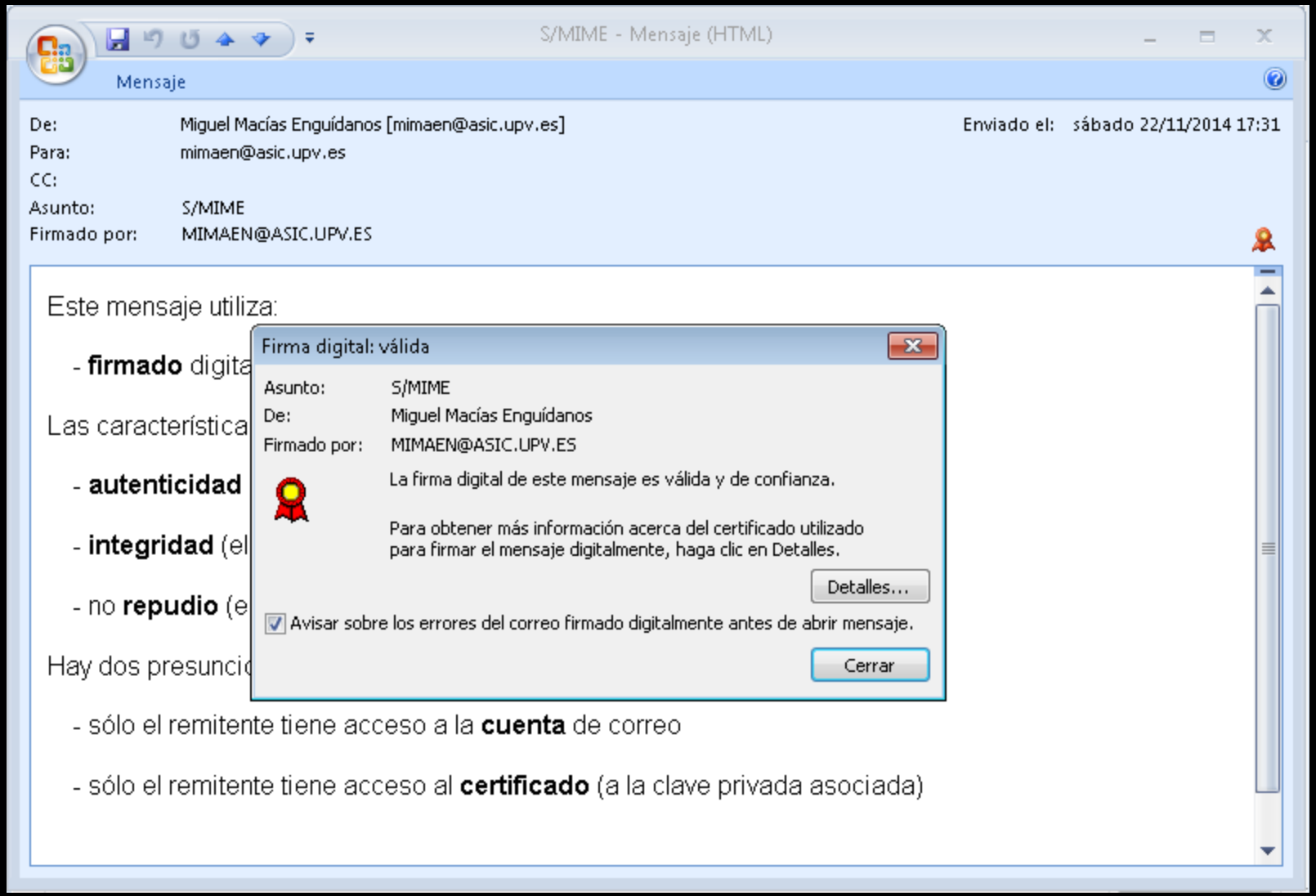
- **firmado** digital

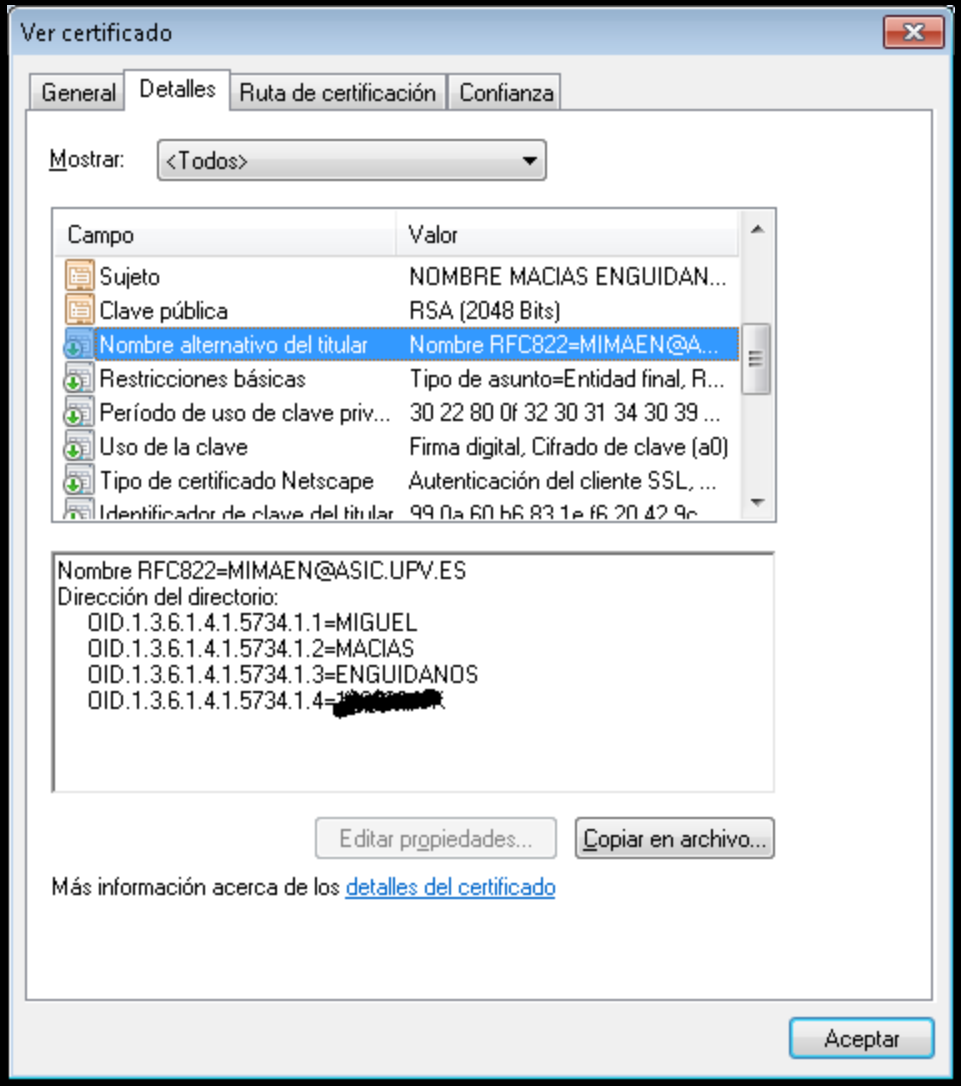
Las características que nos garantiza son:

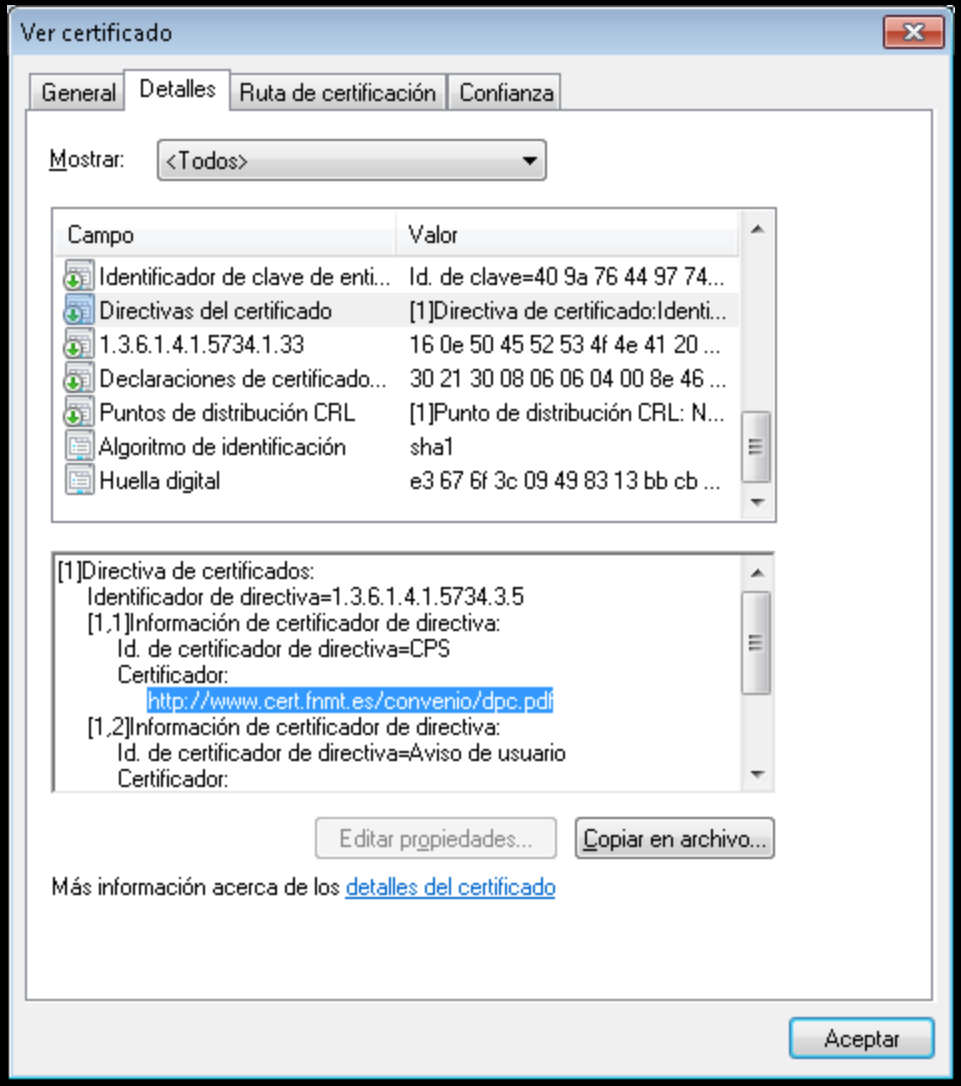
- **autenticidad** (el mensaje sólo lo puede haber enviado el remitente)
- **integridad** (el mensaje no se ha modificado desde que se envió)
- no **repudio** (el remitente no puede negar haber enviado el mensaje)

Hay dos presunciones básicas en este mecanismo:

- sólo el remitente tiene acceso a la **cuenta** de correo
- sólo el remitente tiene acceso al **certificado** (a la clave privada asociada)


S/MIME - Mensaje (HTML)
Mensaje
De: Miguel Macías Enguídanos [mimaen@asic.upv.es]
Enviado el: sábado 22/11/2014 17:31
Para: mimaen@asic.upv.es
CC:
Asunto: S/MIME
Firmado por: MIMAEN@ASIC.UPV.ES
Este mensaje utiliza:
- firmado digita
Las característica
- autenticidad
- integridad (el
- no repudio (e
Hay dos presunci
- sólo el remitente tiene acceso a la cuenta de correo
- sólo el remitente tiene acceso al certificado (a la clave privada asociada)
Firma digital: válida
Asunto: S/MIME
De: Miguel Macías Enguídanos
Firmado por: MIMAEN@ASIC.UPV.ES
La firma digital de este mensaje es válida y de confianza.
Para obtener más información acerca del certificado utilizado para firmar el mensaje digitalmente, haga clic en Detalles.
Detalles...
Avisar sobre los errores del correo firmado digitalmente antes de abrir mensaje.
Cerrar


Ver certificado
General
Detalles
Ruta de certificación
Confianza
Mostrar:
<Todos>
Campo
Valor
Sujeto
NOMBRE MACIAS ENGUIDAN...
Clave pública
RSA (2048 Bits)
Nombre alternativo del titular
Nombre RFC822=MIMAEN@A...
Restricciones básicas
Tipo de asunto=Entidad final, R...
Período de uso de clave priv...
30 22 80 0f 32 30 31 34 30 39 ...
Uso de la clave
Firma digital, Cifrado de clave (a0)
Tipo de certificado Netscape
Autenticación del cliente SSL, ...
Nombre RFC822=MIMAEN@ASIC.UPV.ES
Dirección del directorio:
OID.1.3.6.1.4.1.5734.1.1=MIGUEL
OID.1.3.6.1.4.1.5734.1.2=MACIAS
OID.1.3.6.1.4.1.5734.1.3=ENGUIDANOS
OID.1.3.6.1.4.1.5734.1.4=
Editar propiedades...
Copiar en archivo...
Más información acerca de los detalles del certificado
Aceptar


Ver certificado
General
Detalles
Ruta de certificación
Confianza
Mostrar:
<Todos>
Campo
Valor
Identificador de clave de enti...
Id. de clave=40 9a 76 44 97 74...
Directivas del certificado
[1]Directiva de certificado:Identi...
1.3.6.1.4.1.5734.1.33
16 0e 50 45 52 53 4f 4e 41 20 ...
Declaraciones de certificado...
30 21 30 08 06 06 04 00 8e 46 ...
Puntos de distribución CRL
[1]Punto de distribución CRL: N...
Algoritmo de identificación
sha1
Huella digital
e3 67 6f 3c 09 49 83 13 bb cb ...
[1]Directiva de certificados:
Identificador de directiva=1.3.6.1.4.1.5734.3.5
[1,1]Información de certificador de directiva:
Id. de certificador de directiva=CPS
Certificador:
http://www.cert.fnmt.es/convenio/dpc.pdf
[1,2]Información de certificador de directiva:
Id. de certificador de directiva=Aviso de usuario
Certificador:
Editar propiedades...
Copiar en archivo...
Más información acerca de los detalles del certificado
Aceptar

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

II.2.1.3 Confirmación de la identidad personal

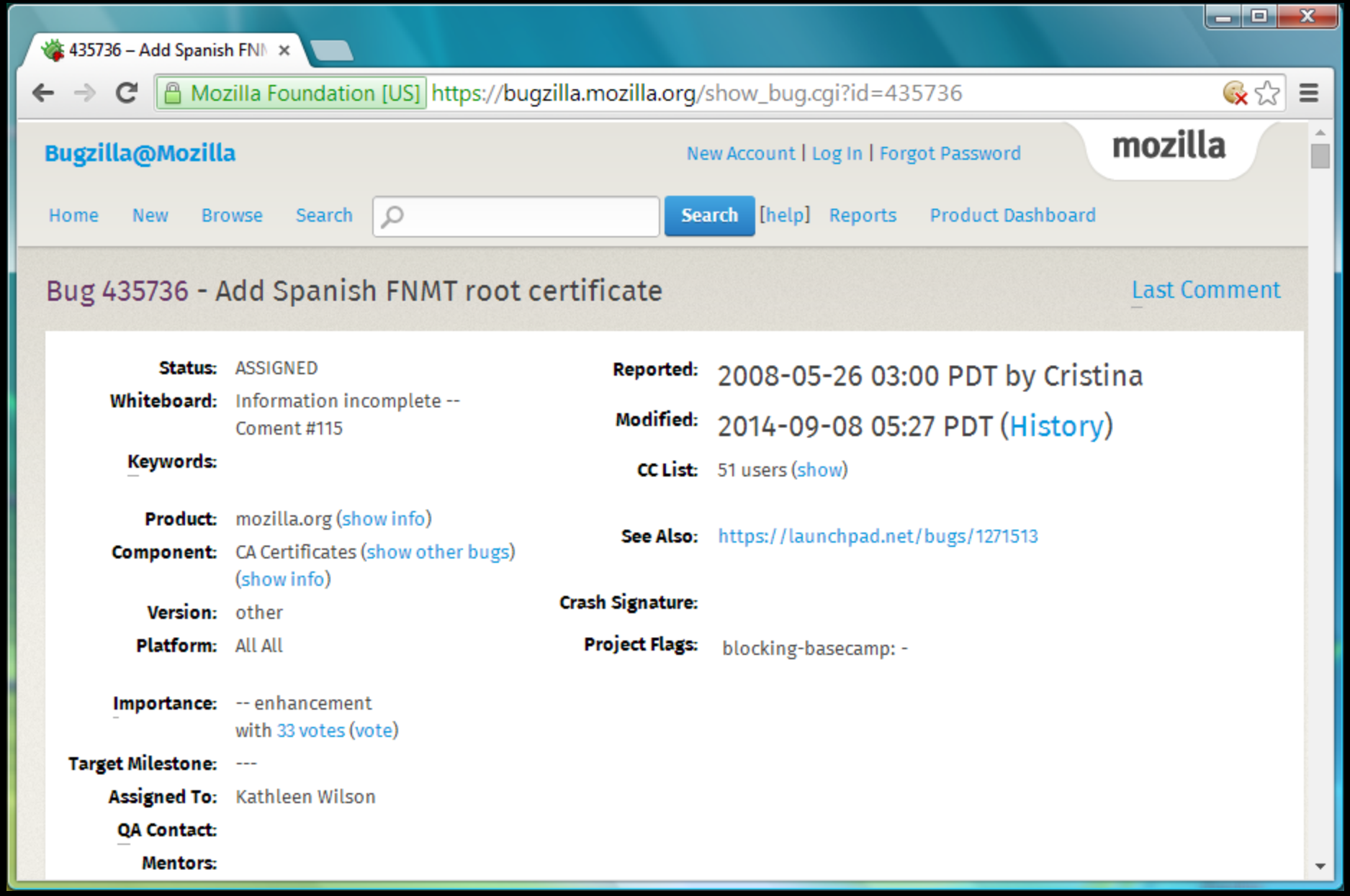
…

los *Solicitantes de Certificados deberán comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, presentándose en la Oficina de Registro autorizada, en posesión de su DNI, válido y vigente,*

II.2.2.2 Composición de la identidad alternativa del *Suscriptor*

…

[1] Por otra parte, además del subcampo *directoryName de la extensión subjectAltName, en el caso de que se haya aportado una dirección de correo electrónico por el Suscriptor durante el proceso de solicitud de emisión del Certificado, ésta estará incluida en el subcampo rfc822Name.*


435736 – Add Spanish FNM
Mozilla Foundation [US] https://bugzilla.mozilla.org/show_bug.cgi?id=435736
Bugzilla@Mozilla
New Account | Log In | Forgot Password
mozilla
Home New Browse Search Search [help] Reports Product Dashboard
Bug 435736 - Add Spanish FNMT root certificate
Last Comment
Status: ASSIGNED
Whiteboard: Information incomplete -- Coment #115
Keywords:
Product: mozilla.org (show info)
Component: CA Certificates (show other bugs) (show info)
Version: other
Platform: All All
Importance: -- enhancement with 33 votes (vote)
Target Milestone: ---
Assigned To: Kathleen Wilson
QA Contact:
Mentors:
Reported: 2008-05-26 03:00 PDT by Cristina
Modified: 2014-09-08 05:27 PDT (History)
CC List: 51 users (show)
See Also: https://launchpad.net/bugs/1271513
Crash Signature:
Project Flags: blocking-basecamp: -

Cristina 2008-12-01 04:14:51 PST

b) for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf;

"The main purpose of certificates issued by FNMT-RCM Certification Authority is user identity authentication nor digitally sign and/or encryption email messages. The email is only used as contact method to send information to users".

Rafa 2009-10-19 10:53:55 PDT

> Then the requested trust bits should not include email (S/MIME). The requested
> trust bits should only be websites (SSL/TLS) and Code Signing, not email. Do
> you agree?

We're agree. Nevertheless, it would be interesting for future uses that trust bits include email.

S/MIME - Mensaje (HTML)

Mensaje

De: Miguel Macías Enguídanos [mimaen@asic.upv.es]
Para: mimaen@asic.upv.es
CC:
Asunto: S/MIME
Firmado por: MIMAEN@ASIC.UPV.ES

Enviado el: sábado 22/11/2014 17:31

Este mensaje utiliza:

- **firmado** digital

Las características que nos garantiza son:

- **autenticidad** (el mensaje sólo lo puede haber enviado el remitente)
- **integridad** (el mensaje no se ha modificado desde que se envió)
- no **repudio** (el remitente no puede negar haber enviado el mensaje)

Hay dos presunciones básicas en este mecanismo:

- sólo el remitente tiene acceso a la **cuenta** de correo
- sólo el remitente tiene acceso al **certificado** (a la clave privada asociada)

Persona Física
Obtener Certificado Software
Obtener Certificado en Tarjeta
Obtener Certificado con Android
Obtener Certificado con DNIe
Verificar estado
Solicitar verificación
Renovar
Modificar datos
Anular
Persona Jurídica
Entidad Sin Personalidad Jurídica
Administración Pública

Verificar estado

Estimado Sr/Sra. MACIAS.

Su certificado acaba de ser verificado. Esta usted en disposición de un Certificado Digital **REVOCADO**.

Información sobre la identidad (Valores Personales)

Identificador	Valor
Nombre	MIGUEL
Primer apellido	MACIAS
Segundo apellido	ENGUIDANOS
NIF	***NIF***
Dirección de Correo Electrónico	MIMAEN@ASIC.UPV.ES

Información sobre las claves (Valores Técnicos)

Identificador	Valor
Numero de Serie del Certificado	1025311101

Fecha y Hora Oficial

22/11/2014

19:11:22

Soporte Técnico

https://valide.redsara.es/valide/verDetalleCertificado/ejecutar.html

.gob.es VALIDe

Contactar

Bienvenido | Benvingut | Ongi etorri | Benvido | Welcome

GOBIERNO DE ESPAÑA

- Validar Certificado
- Realizar firma
- Validar Firma
- Validar Sede Electrónica
- Visualizar Firma
- Faqs

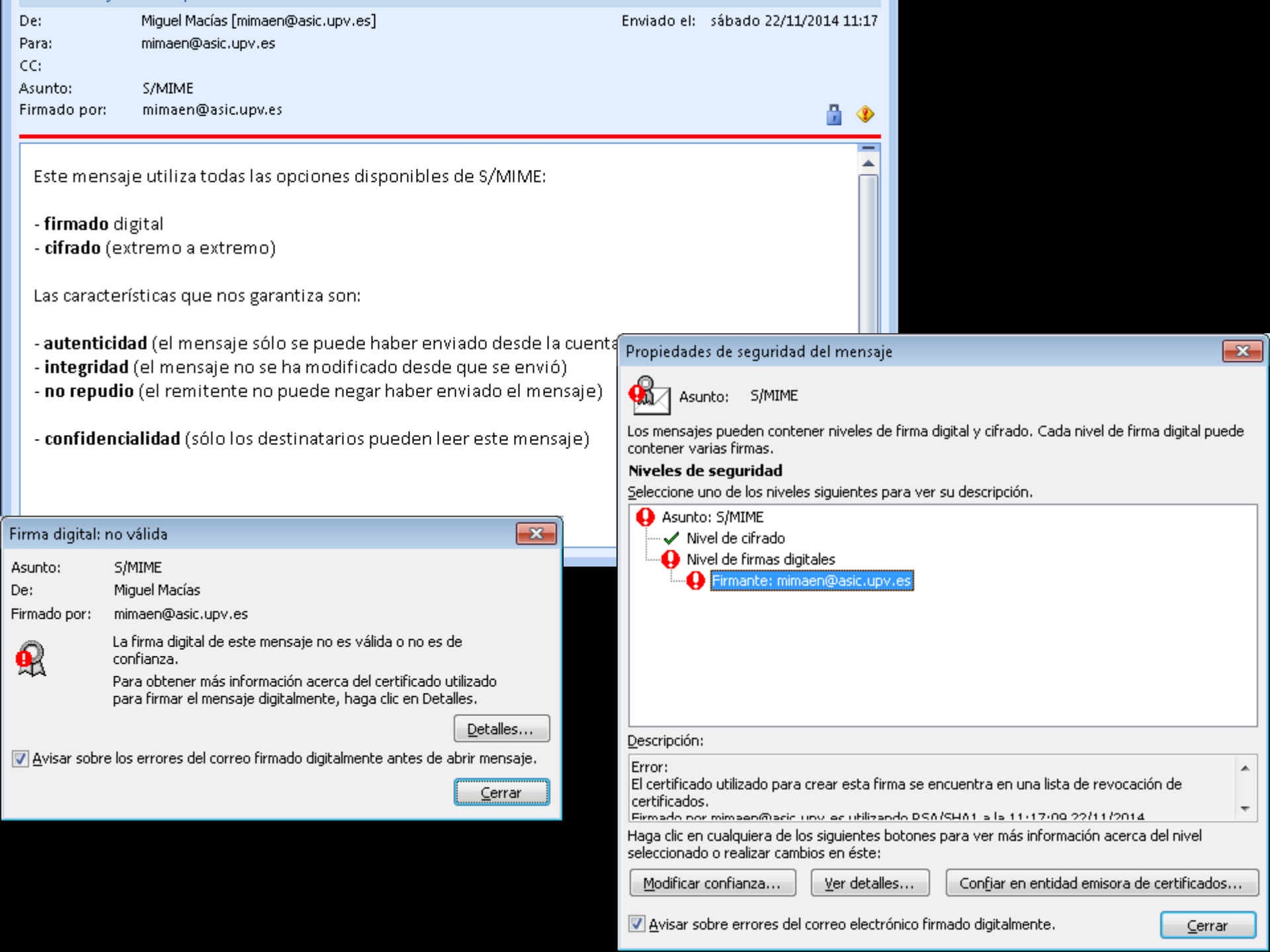
Resultado de Validar Certificado

Certificado inválido
El certificado se encuentra revocado

Nombre/Apellid. Responsable: MIGUEL MACIAS ENGUIDANOS
NIF Responsable: ***NIF***

Información del certificado

Apellidos del responsable: MACIAS ENGUIDANOS
Clasificación: 0
Email: MIMAEN@ASIC.UPV.ES
ID Emisor: OU=FNMT Clase 2 CA,O=FNMT,C=ES
ID Política: MITyC
NIF Responsable: ***NIF***
Nombre/Apellid. Responsable: MIGUEL MACIAS ENGUIDANOS
Nombre del responsable: MIGUEL
Número de serie: 1025311101
Organización emisora: FNMT
Política: 1.3.6.1.4.1.5734.3.5


De: Miguel Macías [mimaen@asic.upv.es]
Enviado el: sábado 22/11/2014 11:17
Para: mimaen@asic.upv.es
CC:
Asunto: S/MIME
Firmado por: mimaen@asic.upv.es
Este mensaje utiliza todas las opciones disponibles de S/MIME:
- firmado digital
- cifrado (extremo a extremo)
Las características que nos garantiza son:
- autenticidad (el mensaje sólo se puede haber enviado desde la cuenta
- integridad (el mensaje no se ha modificado desde que se envió)
- no repudio (el remitente no puede negar haber enviado el mensaje)
- confidencialidad (sólo los destinatarios pueden leer este mensaje)
Firma digital: no válida
Asunto: S/MIME
De: Miguel Macías
Firmado por: mimaen@asic.upv.es
La firma digital de este mensaje no es válida o no es de confianza.
Para obtener más información acerca del certificado utilizado para firmar el mensaje digitalmente, haga clic en Detalles.
Detalles...
Avisar sobre los errores del correo firmado digitalmente antes de abrir mensaje.
Cerrar
Propiedades de seguridad del mensaje
Asunto: S/MIME
Los mensajes pueden contener niveles de firma digital y cifrado. Cada nivel de firma digital puede contener varias firmas.
Niveles de seguridad
Seleccione uno de los niveles siguientes para ver su descripción.
Asunto: S/MIME
Nivel de cifrado
Nivel de firmas digitales
Firmante: mimaen@asic.upv.es
Descripción:
Error:
El certificado utilizado para crear esta firma se encuentra en una lista de revocación de certificados.
Haga clic en cualquiera de los siguientes botones para ver más información acerca del nivel seleccionado o realizar cambios en éste:
Modificar confianza...
Ver detalles...
Confiar en entidad emisora de certificados...
Avisar sobre errores del correo electrónico firmado digitalmente.
Cerrar

De Miguel Macías <mimaen@asic.upv.es>

Asunto **S/MIME**

22/11/2014 11:17

A mimaen@asic.upv.es

Otras acciones

Este mensaje utiliza todas las opciones disponibles de S/MIME:

- **firmado** digital
- **cifrado** (extremo a extremo)

Las características que nos garantiza son:

- **autenticidad** (el mensaje sólo se puede haber enviado desde la cuenta remitente)
- **integridad** (el mensaje no se ha modificado desde que se envió)
- **no repudio** (el remitente no puede negar haber enviado el mensaje)

- **confidencialidad** (sólo los destinatarios pueden leer este mensaje)

Seguridad del mensaje

La firma digital no es válida

El mensaje incluye una firma digital, pero la firma no es válida.

El certificado utilizado para firmar el mensaje fue emitido por una Autoridad Certificadora (CA) en la que no confía para emitir este tipo de certificado.

Firmado por:

Direcciones de correo electrónico: mimaen@asic.upv.es

Certificado emitido por: COMODO RSA Client Authentication and Secure Email

Ver certificado de la firma

El mensaje está cifrado

Este mensaje fue cifrado antes de ser enviado. El cifrado hace muy difícil que otras personas puedan ver información mientras ésta viaja por la red.

Acepta

Visor de certificados:"mimaen"

General Detalles

No se pudo verificar este certificado porque ha sido revocado.

Emitido para

Nombre común (CN)	<No es parte de un certificado>
Organización (O)	<No es parte de un certificado>
Unidad organizativa (OU)	<No es parte de un certificado>
Número de serie	00:D8:E8:AE:D6:21:78:70:3B:56:6D:E8:FF:02:EA:F7:B3

Emitido por

Nombre común (CN)	COMODO RSA Client Authentication and Secure Email CA
Organización (O)	COMODO CA Limited
Unidad organizativa (OU)	<No es parte de un certificado>

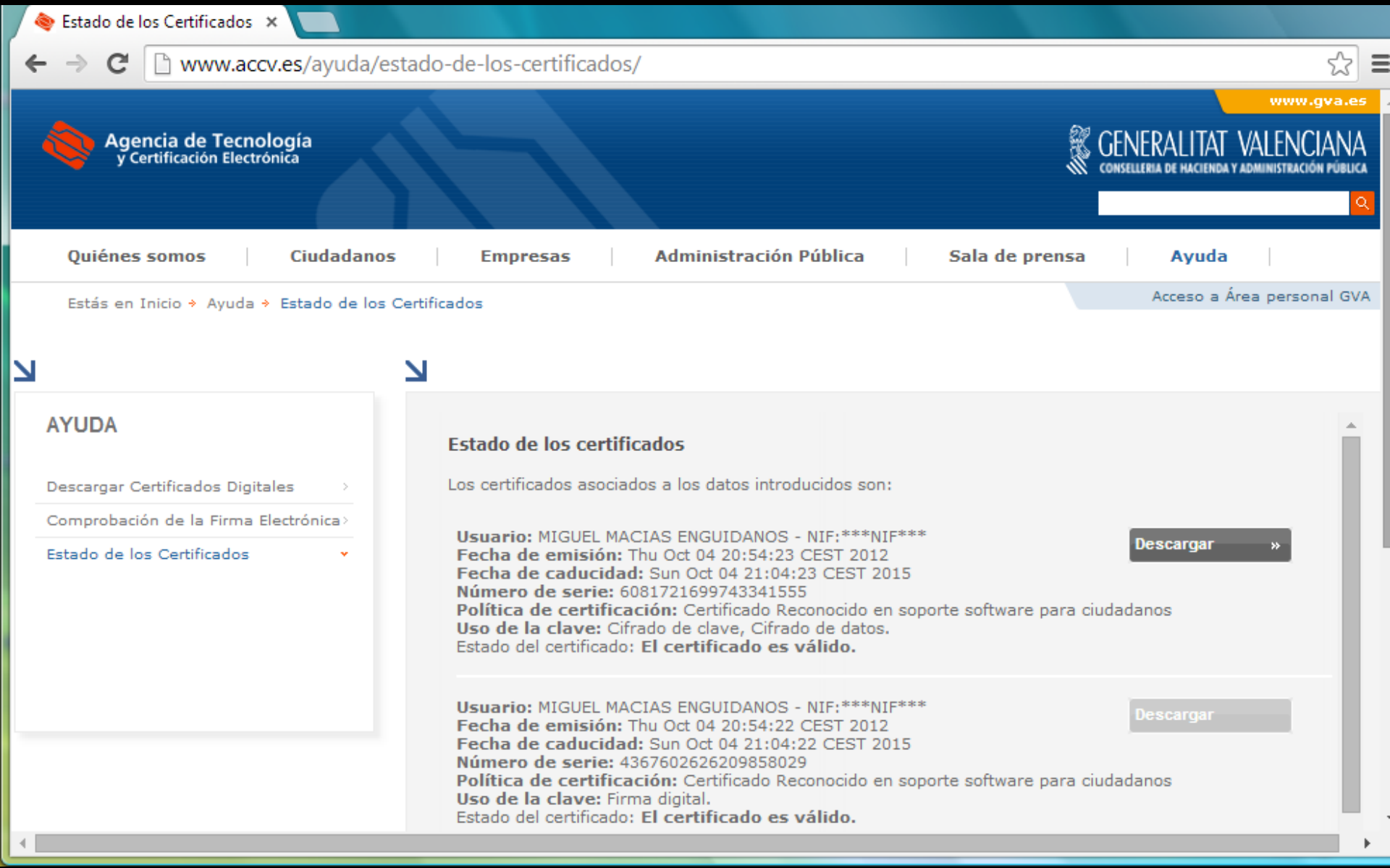
Periodo de validez

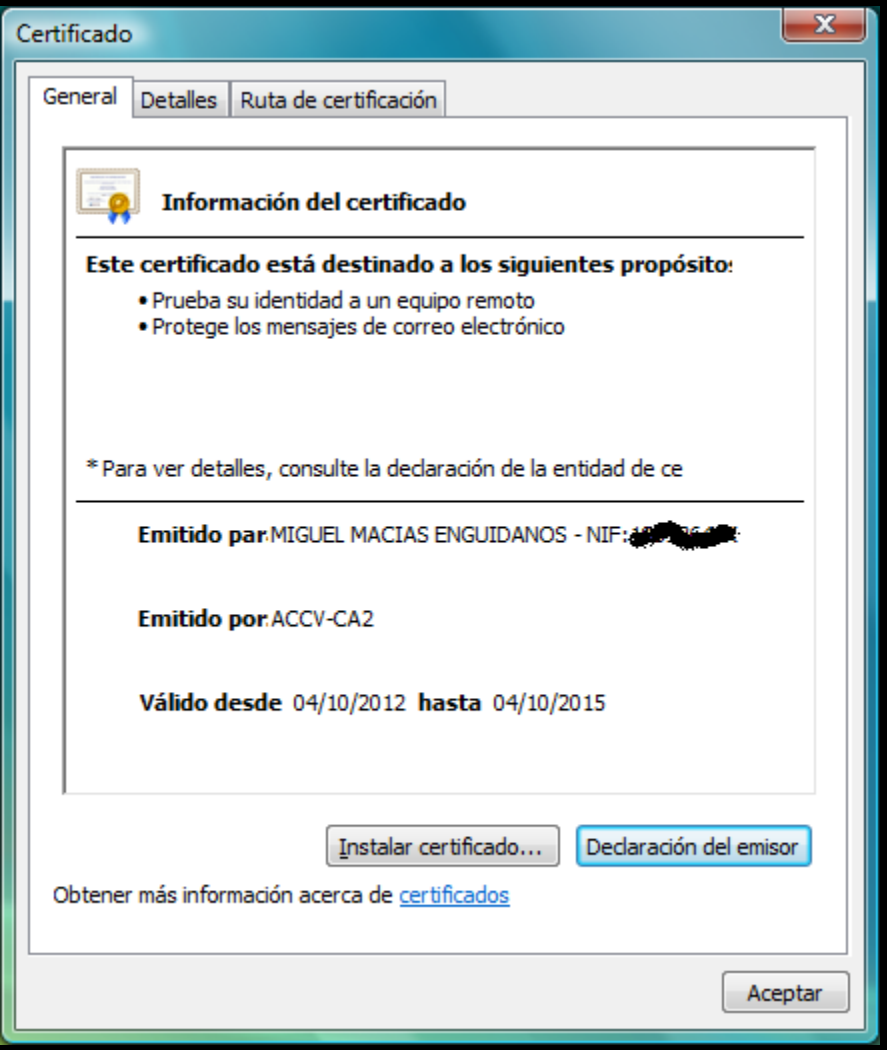
Comienza el	22/11/2014
Caduca el	23/11/2015

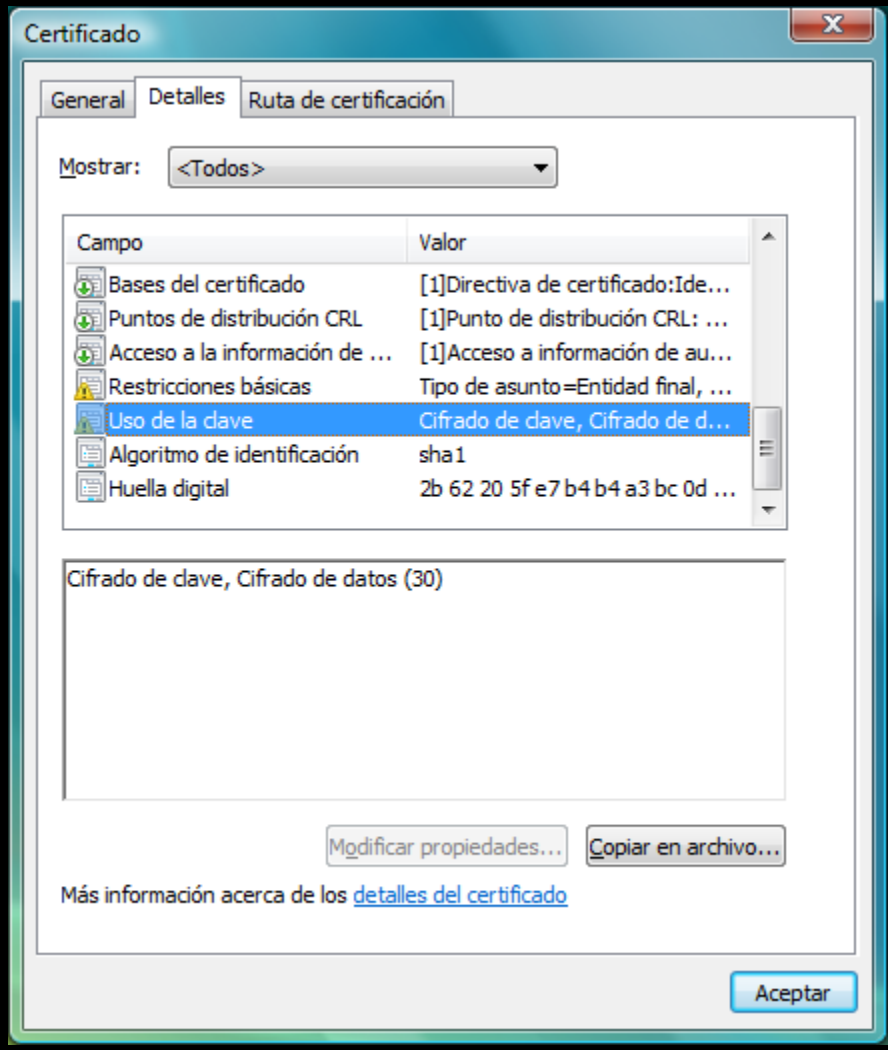
Huellas digitales

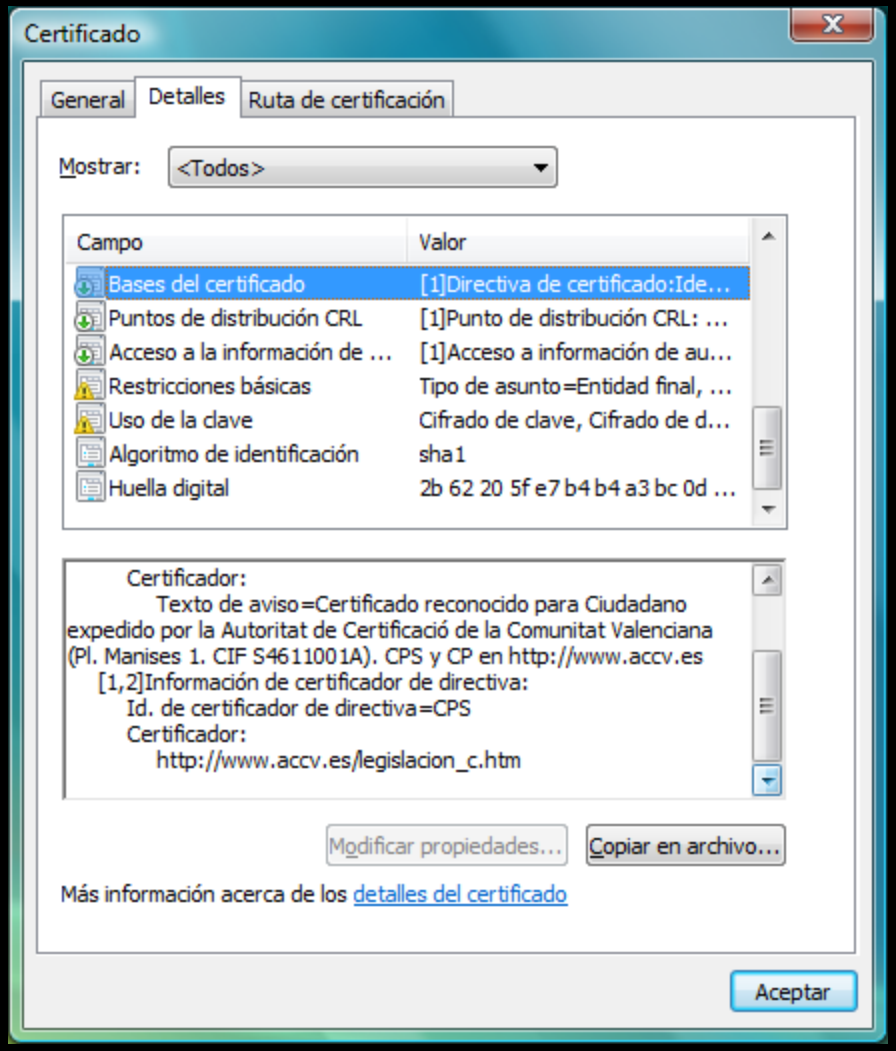
Huella digital SHA1	16:00:F8:7D:4C:6B:13:64:D4:6A:F6:B5:84:0D:3B:27:14:E3:D8:DD
Huella digital MD5	ED:7F:12:9D:C3:09:73:4D:BB:0C:50:B7:30:D3:29:2A

4


Estado de los Certificados
www.accv.es/ayuda/estado-de-los-certificados/
www.gva.es
Agencia de Tecnología y Certificación Electrónica
GENERALITAT VALENCIANA
CONSELLERIA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA
Quiénes somos | Ciudadanos | Empresas | Administración Pública | Sala de prensa | Ayuda
Estás en Inicio → Ayuda → Estado de los Certificados
Acceso a Área personal GVA
AYUDA
Descargar Certificados Digitales
Comprobación de la Firma Electrónica
Estado de los Certificados
Estado de los certificados
Los certificados asociados a los datos introducidos son:
Usuario: MIGUEL MACIAS ENGUIDANOS - NIF:***NIF***
Fecha de emisión: Thu Oct 04 20:54:23 CEST 2012
Fecha de caducidad: Sun Oct 04 21:04:23 CEST 2015
Número de serie: 6081721699743341555
Política de certificación: Certificado Reconocido en soporte software para ciudadanos
Uso de la clave: Cifrado de clave, Cifrado de datos.
Estado del certificado: El certificado es válido.
Descargar
Usuario: MIGUEL MACIAS ENGUIDANOS - NIF:***NIF***
Fecha de emisión: Thu Oct 04 20:54:22 CEST 2012
Fecha de caducidad: Sun Oct 04 21:04:22 CEST 2015
Número de serie: 4367602626209858029
Política de certificación: Certificado Reconocido en soporte software para ciudadanos
Uso de la clave: Firma digital.
Estado del certificado: El certificado es válido.
Descargar


Certificado
General
Detalles
Ruta de certificación
Información del certificado
Este certificado está destinado a los siguientes propósito:
• Prueba su identidad a un equipo remoto
• Protege los mensajes de correo electrónico
* Para ver detalles, consulte la declaración de la entidad de ce
Emitido par: MIGUEL MACIAS ENGUIDANOS - NIF:
Emitido por: ACCV-CA2
Válido desde 04/10/2012 hasta 04/10/2015
Instalar certificado...
Declaración del emisor
Obtener más información acerca de certificados
Aceptar

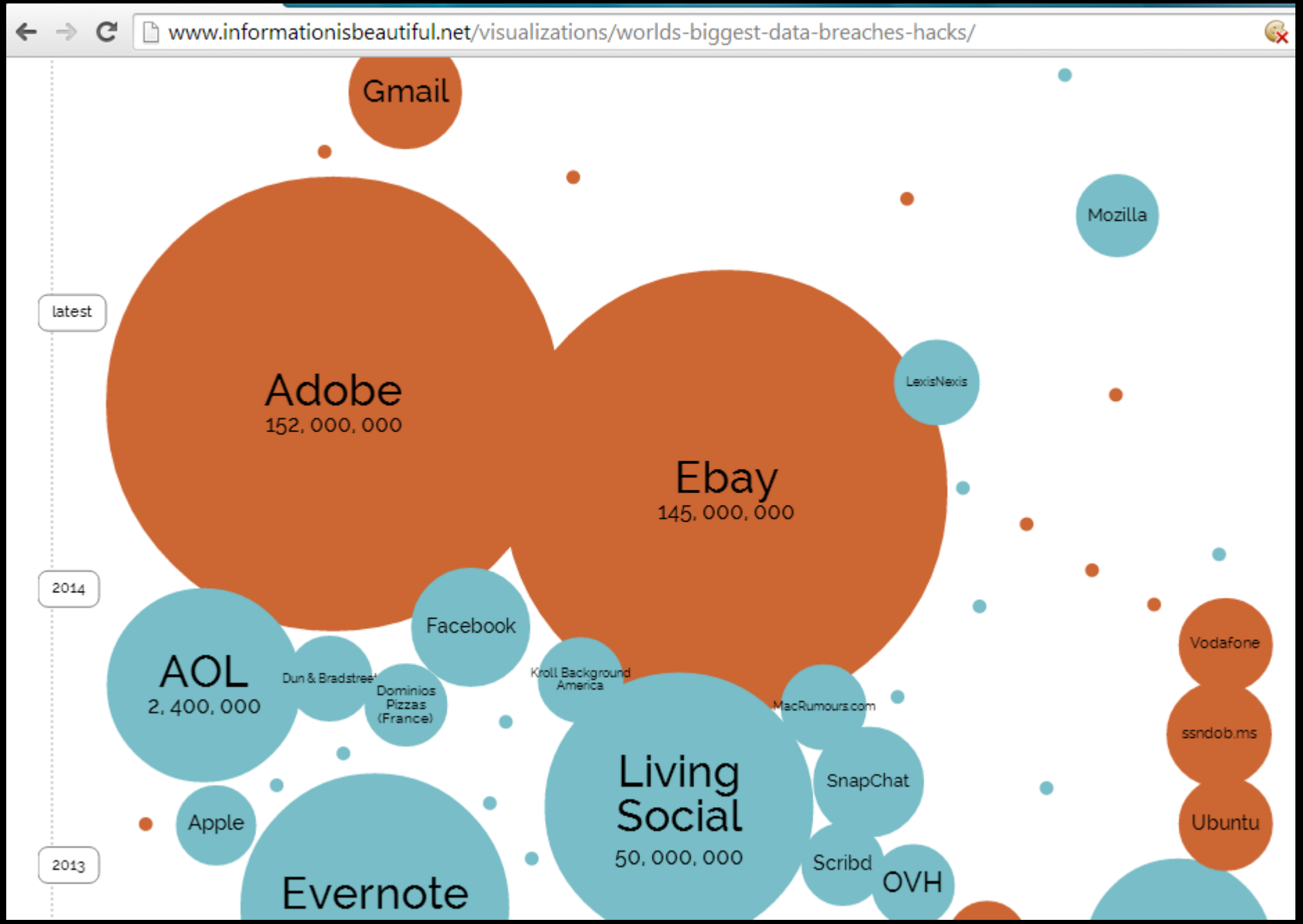

Certificado
General
Detalles
Ruta de certificación
Mostrar: <Todos>
Campo
Valor
Bases del certificado
[1]Directiva de certificado:Ide...
Puntos de distribución CRL
[1]Punto de distribución CRL: ...
Acceso a la información de ...
[1]Acceso a información de au...
Restricciones básicas
Tipo de asunto=Entidad final, ...
Uso de la clave
Cifrado de clave, Cifrado de d...
Algoritmo de identificación
sha1
Huella digital
2b 62 20 5f e7 b4 b4 a3 bc 0d ...
Cifrado de clave, Cifrado de datos (30)
Modificar propiedades...
Copiar en archivo...
Más información acerca de los detalles del certificado
Aceptar


Certificado
General
Detalles
Ruta de certificación
Mostrar:
<Todos>
Campo
Valor
Bases del certificado
[1]Directiva de certificado:Ide...
Puntos de distribución CRL
[1]Punto de distribución CRL: ...
Acceso a la información de ...
[1]Acceso a información de au...
Restricciones básicas
Tipo de asunto=Entidad final, ...
Uso de la clave
Cifrado de clave, Cifrado de d...
Algoritmo de identificación
sha1
Huella digital
2b 62 20 5f e7 b4 b4 a3 bc 0d ...
Certificador:
Texto de aviso=Certificado reconocido para Ciudadano expedido por la Autoritat de Certificació de la Comunitat Valenciana (Pl. Manises 1. CIF S4611001A). CPS y CP en http://www.accv.es
[1,2]Información de certificador de directiva:
Id. de certificador de directiva=CPS
Certificador:
http://www.accv.es/legislacion_c.htm
Modificar propiedades...
Copiar en archivo...
Más información acerca de los detalles del certificado
Aceptar

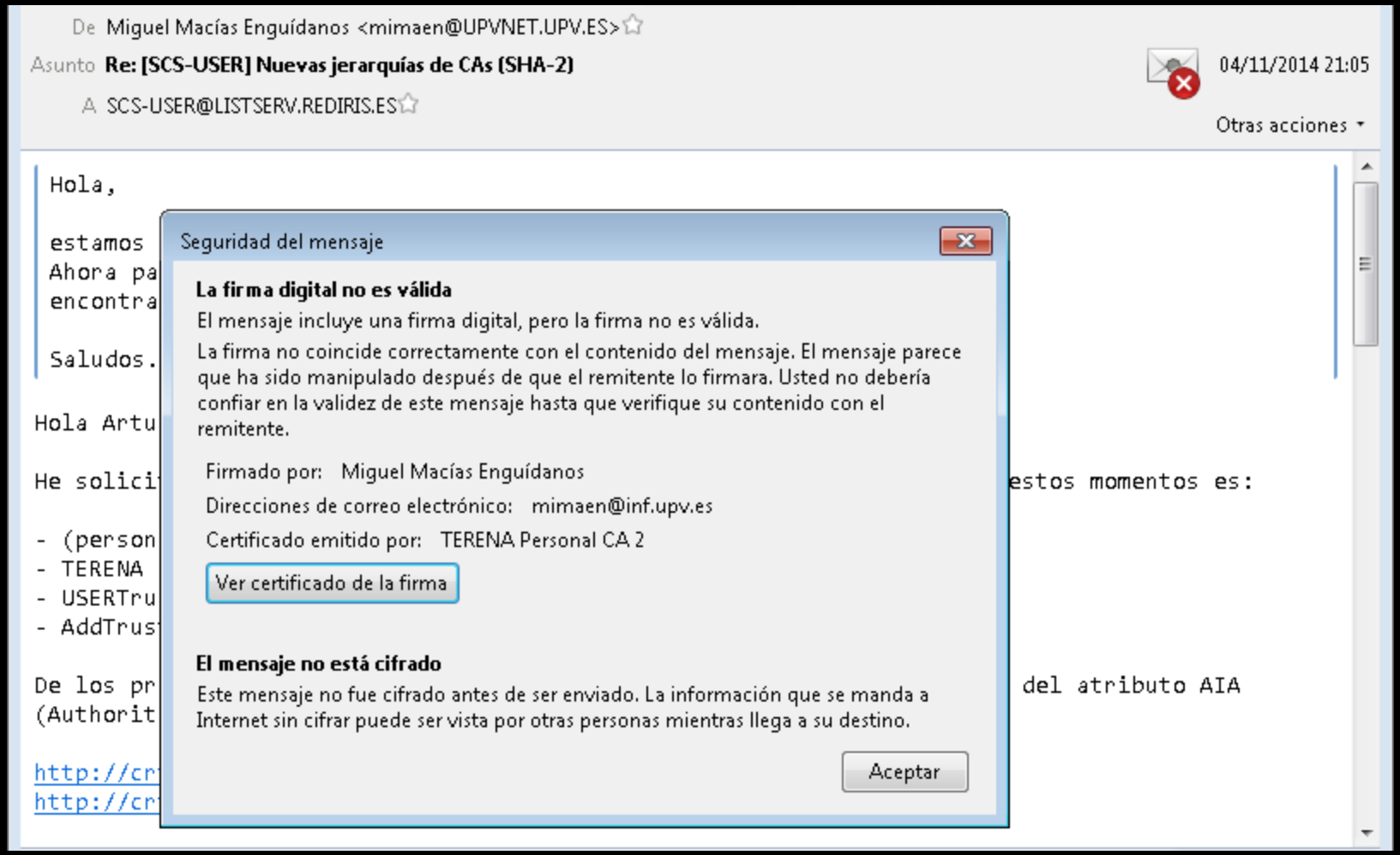
Política de Certificación de Certificados reconocidos en soporte software para ciudadanos

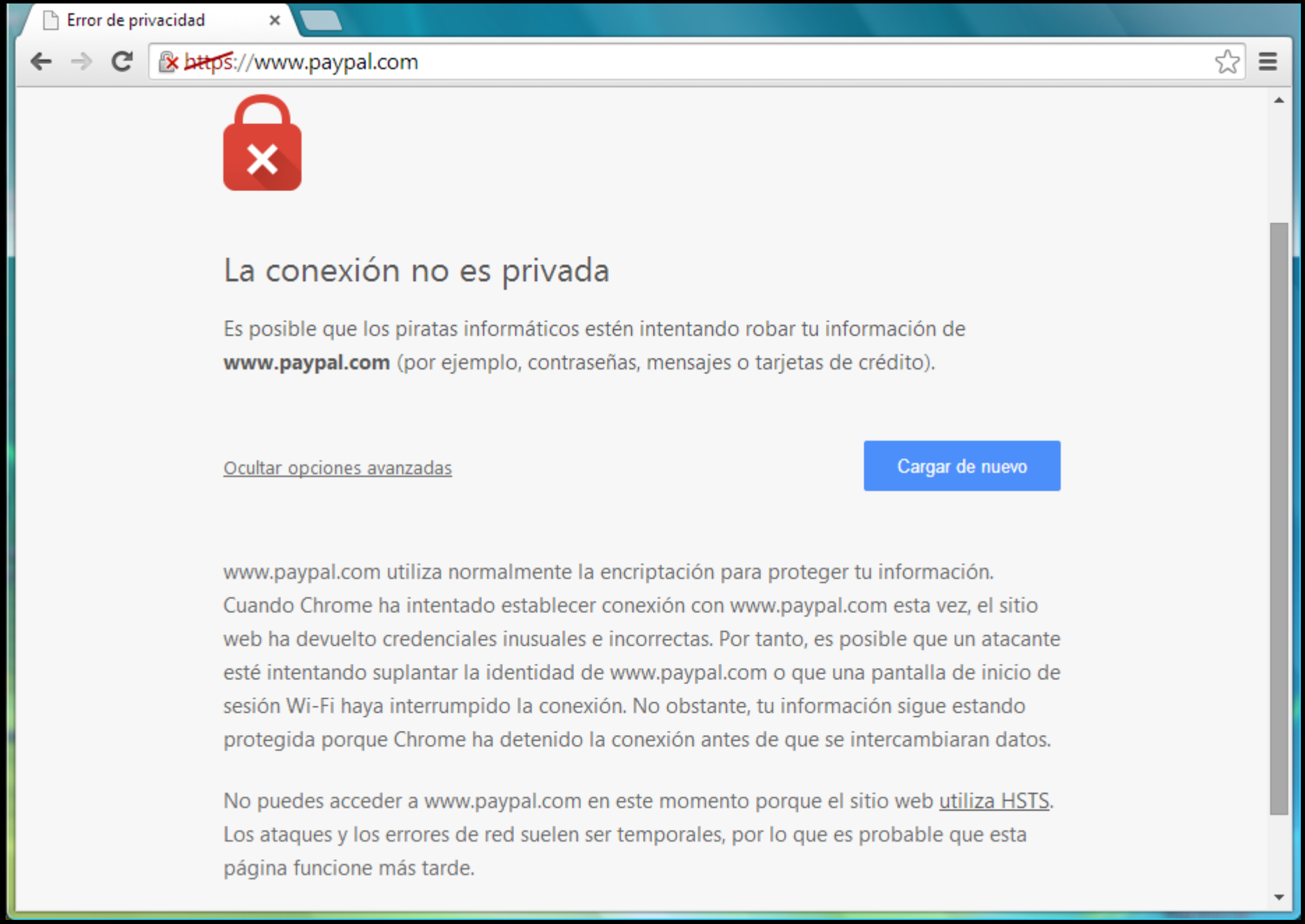
4.12. Depósito y recuperación de claves.

La ACCV realiza el depósito de certificados y claves de cifrado para permitir la recuperación de informaciones cifradas en caso de pérdida de las claves necesarias para su descifrado, por interés legítimo del titular de los certificados o por requerimiento judicial.


www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Gmail
Mozilla
latest
Adobe
152, 000, 000
Ebay
145, 000, 000
LexisNexis
2014
AOL
2, 400, 000
Dun & Bradstreet
Dominios Pizzas (France)
Facebook
Kroll Background America
MacRumours.com
Vodafone
ssndob.ms
Living Social
50, 000, 000
SnapChat
Ubuntu
Apple
2013
Evernote
Scribd
OVH

5


De Miguel Macías Enguídanos <mimaen@UPVNET.UPV.ES>
Asunto Re: [SCS-USER] Nuevas jerarquías de CAs (SHA-2)
A SCS-USER@LISTSERV.REDIRIS.ES
04/11/2014 21:05
Otras acciones
Hola,
estamos
Ahora pa
encontra
Saludos.
Hola Artu
He solici
estos momentos es:
- (person
- TERENA
- USERTru
- AddTrus
De los pr
del atributo AIA
(Authorit
http://cr
http://cr
Seguridad del mensaje
La firma digital no es válida
El mensaje incluye una firma digital, pero la firma no es válida.
La firma no coincide correctamente con el contenido del mensaje. El mensaje parece que ha sido manipulado después de que el remitente lo firmara. Usted no debería confiar en la validez de este mensaje hasta que verifique su contenido con el remitente.
Firmado por: Miguel Macías Enguídanos
Direcciones de correo electrónico: mimaen@inf.upv.es
Certificado emitido por: TERENA Personal CA 2
Ver certificado de la firma
El mensaje no está cifrado
Este mensaje no fue cifrado antes de ser enviado. La información que se manda a Internet sin cifrar puede ser vista por otras personas mientras llega a su destino.
Aceptar


Error de privacidad
https://www.paypal.com
La conexión no es privada
Es posible que los piratas informáticos estén intentando robar tu información de **www.paypal.com** (por ejemplo, contraseñas, mensajes o tarjetas de crédito).
Ocultar opciones avanzadas
Cargar de nuevo
www.paypal.com utiliza normalmente la encriptación para proteger tu información. Cuando Chrome ha intentado establecer conexión con www.paypal.com esta vez, el sitio web ha devuelto credenciales inusuales e incorrectas. Por tanto, es posible que un atacante esté intentando suplantar la identidad de www.paypal.com o que una pantalla de inicio de sesión Wi-Fi haya interrumpido la conexión. No obstante, tu información sigue estando protegida porque Chrome ha detenido la conexión antes de que se intercambiaran datos.
No puedes acceder a www.paypal.com en este momento porque el sitio web utiliza HSTS. Los ataques y los errores de red suelen ser temporales, por lo que es probable que esta página funcione más tarde.

S/MIME