

SCS en la UPC

esCERT-UPC

Elena Galván Fernández

19 de Noviembre 2007



Índice

- Precedente
- Certificados con RedIRIS
 - Motivación y ventajas
- Nueva gestión
 - Documentación PROXY-SCS
 - Información para los administradores
 - Certificado digital
 - Primera etapa de testeo
 - Entorno
- Paso a paso



Precedente

- esCERT-UPC realizaba gestiones como Autoridad de Certificación en un ámbito restringido a la UPC.
- Caducidad CA actual
 - CA propia
 - 144 certificados emitidos
- Se acordó realizar los certificados a través de RedIRIS
 - La única opción viable era a través de correos firmados





Certificados con RedIRIS



cert@escert.upc.edu

**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**

Motivación

- Gestiones digitales
- Posibilidad de centralización
- Ventajas publicadas por RedIRIS
 - Instalación de la CA raíz en los navegadores
 - Menor problemática para los usuarios
 - Eliminamos "problema" Internet Explorer 7.
 - Implicaciones legales
 - Simplicidad de procedimientos
 - Precio gratuito para las instituciones afiliadas a RedIRIS

Ventajas SMIME

- Elevado número de certificados
- Evitamos
 - Retardos
 - Pérdidas de fax
 - Problemas de fax
 - XXX de firma
- Control en el mismo gestor de correo
- Evitamos imprimir documentos innecesarios





Nueva Gestión

Documentación PROXY-SCS

Información para los administradores

Certificado digital

Primera etapa de testeo

Problemas de validación

Validación y mejor organización

Entorno

CutePDF



cert@escert.upc.edu

**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**

Nueva gestión

- En poco más de 1 mes (iiiAGOSTO!!!) se tenía que realizar toda la gestión
 - Actualización 144 certificados
- Ponernos en contacto con Dani García y su equipo
 - Envío de la documentación de PROXY-SCS por parte del PER
 - Primera etapa de testeo
- Aviso a administradores sobre el cambio
- Reclamar peticiones por Unidades Estructurales
 - Re-reclamar....
- Realización del step-by-step

Documentación PROXY-SCS

- El convenio entre esCERT-UPC y la UPC establece que esCERT-UPC gestionará la realización de los certificados para servidores dentro de la comunidad
- RedIRIS establece que la petición debe ir firmada por el PER de la UPC
- Envío del documento Delegación de Responsabilidad a RedIRIS
 - Proxy1: Elena Galván

Certificados de servidor SCS

Delegación de Responsabilidad – v: 1.0 – 20071111

Yo,

_____, con D.N.I. _____, PER de

AUTORIZO a las personas listadas a continuación a que soliciten y validen en mi nombre los certificados SCS ante la autoridad de registro operada por RedIRIS para este servicio, utilizando para ello cualquier método de identificación electrónico reconocido por la legislación española.

Proxy	Nombre	Apellidos
1	DNI	Email
	Subject DN	
	Autoridad de Certificación	
	Proxy	Nombre



cert@escert.upc.edu

**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**

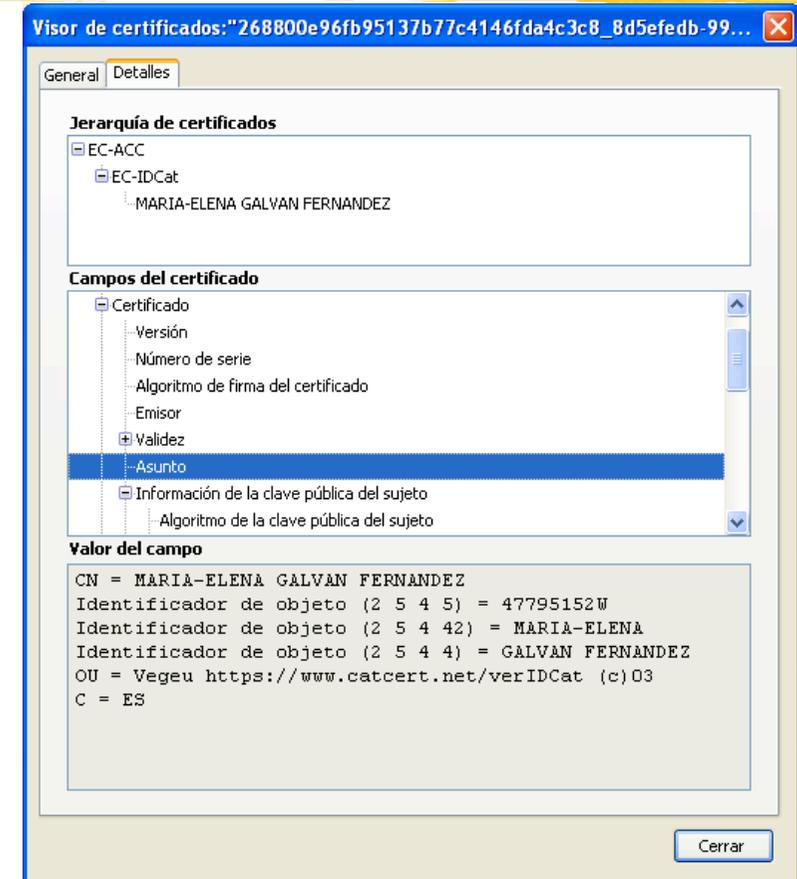
Información para los administradores

- Nueva CA
 - Ventajas
 - Información y Manual de instalación
- Peticiones con alias
 - Minimizar el número de peticiones
- Revocación de certificados



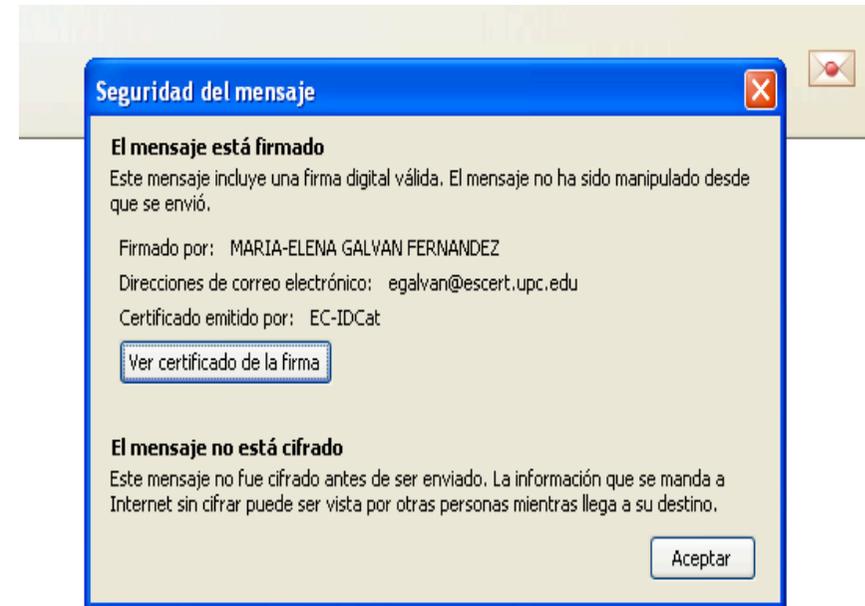
Certificado digital

- Envío del certificado del PROXY a RedIRIS
- idCAT
 - certificado reconocido de identificación y firma electrónica avanzada
 - certificado reconocido de acuerdo con lo que establece el artículo 11.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículos 12, 13, 18 y 20 de dicha Ley



Primera etapa de testeo

- Durante el testeo fueron y vinieron unos cuantos mails....
- Correos con PDF's con .eml's, con .odt, ...
 - **El primer acuerdo fue enviar todo en formato PDF**
- Correos sin firmar
 - Despiste!
- PDF's firmados pero el correo sin firmar



Problemas de validación

- Empezaron los envíos de la documentación y llegó un DdCU con unas cuantas peticiones....
- Se envió un correo con muchos adjuntos
- ¡Problemas al validar la firma!
 - Verification failure > 10233:error:21071065:PKCS7 routines:PKCS7_signatureVerify:digest > failure:pk7_doit.c:928: > 10233:error:21075069:PKCS7 routines:PKCS7_verify:signature > failure:pk7_smime.c:299:
- Solución...

Validación y mejor organización

- Un sólo certificado a realizar – Un sólo mail firmado
 - Asunto correo: [SCS_SMIME][AAAAMMDD.vv] UPC
 - Adjuntos, 3 PDF's:
 - DdCU
 - Paso 3 - CSR
 - Mail GlobalSign - GSmail
- X certificados – X+1 mail's firmados
 - Asunto correo: [SCS-SMIME][AAAAMMDD.vv][CUSO] UPC
 - Adjunto, 1 PDF: DdCU
 - POR CADA CERTIFICADO: Asunto correo: [SCS-SMIME][AAAMMDD.vv][CN]
 - Adjunto, 2 PDF's:
 - Paso 3 - CSR
 - Mail GlobalSign - GSmail



Entorno

- SO Windows XP
- Cliente de correo: Thunderbird 2.0
- PDF's generados con CutePDF
 - <http://www.cutepdf.com/>
 - PDF DdCU
 - PDF CSR
 - PDF GSmail



cert@escert.upc.edu

**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**

CutePDF Writer

- Gratuito
- Paso intermedio PS2PDF
 - Recomendado Ghostscript 8.15
- Añade una nueva impresora
- Imprime desde cualquier formato a PDF





Paso a paso



cert@escert.upc.edu

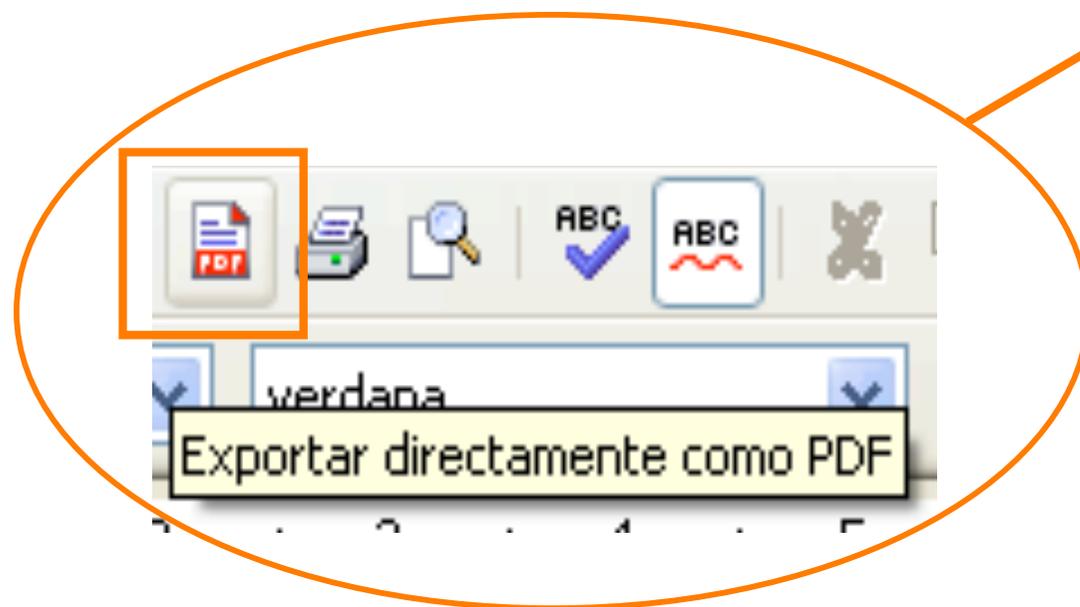
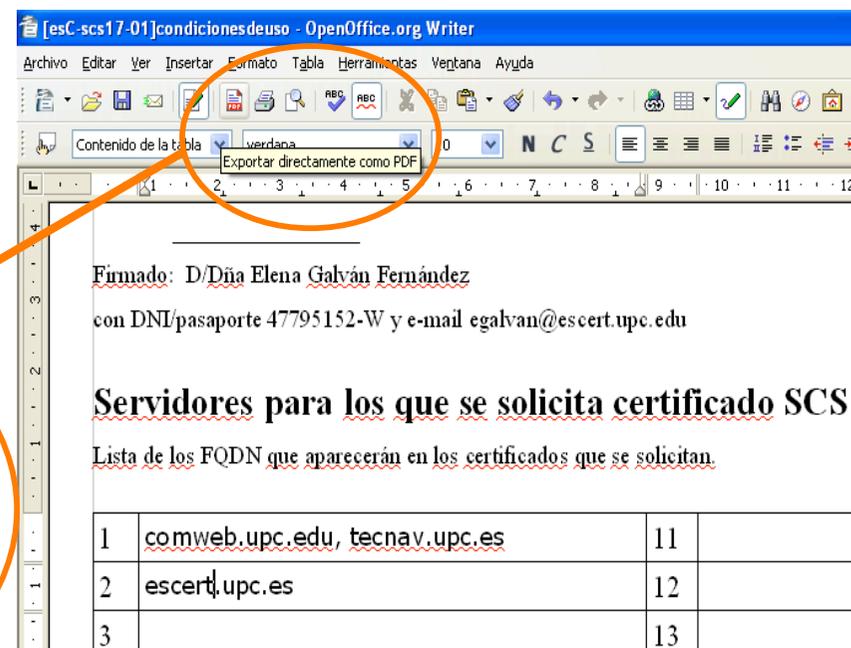
**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**

Paso a Paso

- Documento de Condiciones de Uso
- Aplicación de GlobalSign
 - Incorporación de datos del servidor. Go to Step 2
 - Incorporación de datos del responsable y contacto técnico. Go to Step 3
 - Imprimir paso 3
 - Verificar impresión
 - Clicar en el botón
- Recibir correo de GlobalSign
 - Imprimirlo
- Enviar la documentación a scs-ra@rediris.es

DdCU

- Rellenar documento .odt con los CN
 - Incorporar también los subjectAltName
- Exportar a PDF



Aplicación GlobalSign (1/4)

1. Options

No. Years: 1 year 2 years 3 years

Type of Server Certificate:

Webserver Type:

2. Certificate Request File (CSR)

You can do a copy & paste. Open the CSR in a text editor:

1. Locate the section in the file that looks like

```
-----BEGIN CERTIFICATE REQUEST-----  
(...)  
-----END CERTIFICATE REQUEST-----
```

2. Paste it in the input field below (including the BEGIN and END-lines).

1. Enter here the Certificate Signing Request (CSR) that you have created.

You can use the 'browse' button below : this activates the standard File Upload dialog box that allows you to select the archive containing the CSR you want to upload.

OR

Aplicación GlobalSign (2/4)

RedIRIS SureServerEDU Certificate Procedure - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

https://www.globalsign.net/jra/terena/rediris/edu.cfm

Últimas noticias RedIRIS - Jornadas T... escert.upc.edu: Just ... Aena.es - Aeropuerto... RedIRIS SureServerE... RedIRIS - Guía Básica ... Introducción a la infor...

RedIRIS SCS Servicio de Certificados de Servidor para la comunidad RedIRIS
Cómo usar este servicio

STEP 2: ENTER INFORMATION

Please fill out the following registration form.
This information will be used to verify the identity of your organization and for administration purposes.
It will not be published in your certificate.

Total Cost: SureServerEDU TLS emailserver - 2 years - 1 licence : 0 EUR

Technical Contact		Organisation Information	
Surname:	Galvan	Admin Contact Person:	Elena Galván Fernández
First Name:	Elena	Email:	egalvan@escert.upc.edu
Function:	technical contact	Organization:	UPC
Organization:	UPC	Street & number:	C/Jordi Girona, modul D6-007
Phone number:	934015795	Zip Post Code (optional):	08034
Email:	egalvan@escert.upc.edu	City:	Barcelona
<small>The technical contact is the person who is authorised to run and maintain your secure webserver. This may be your organisation's webmaster or the appropriate technical support staff at your Internet Service Provider (ISP).</small>		Country:	ES
		Phone number:	934015795
		Trade Register No. (optional):	esC-scs15-03.01
		Fax number (optional):	
		DUNS No. (optional):	

Terminado

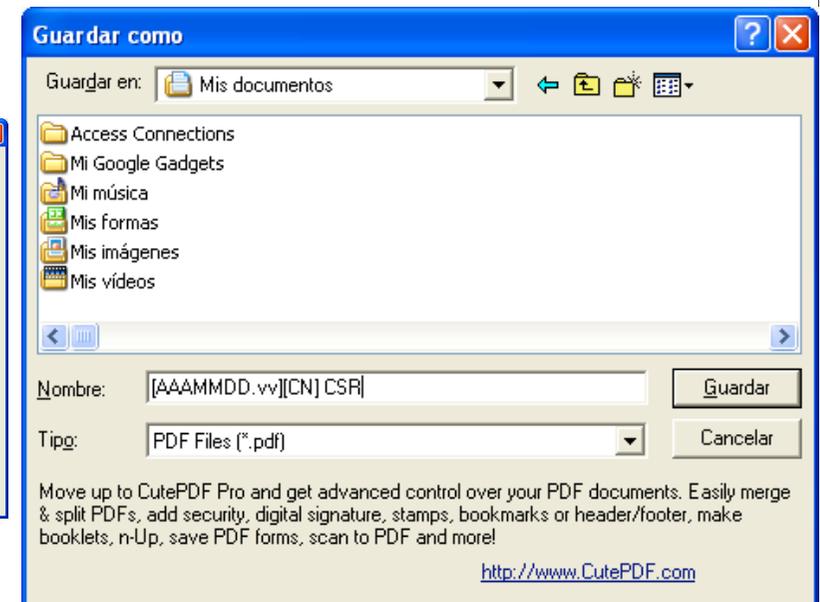
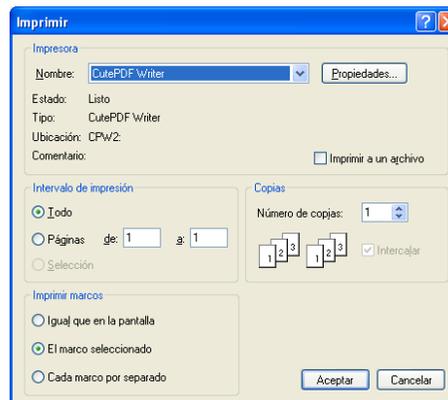
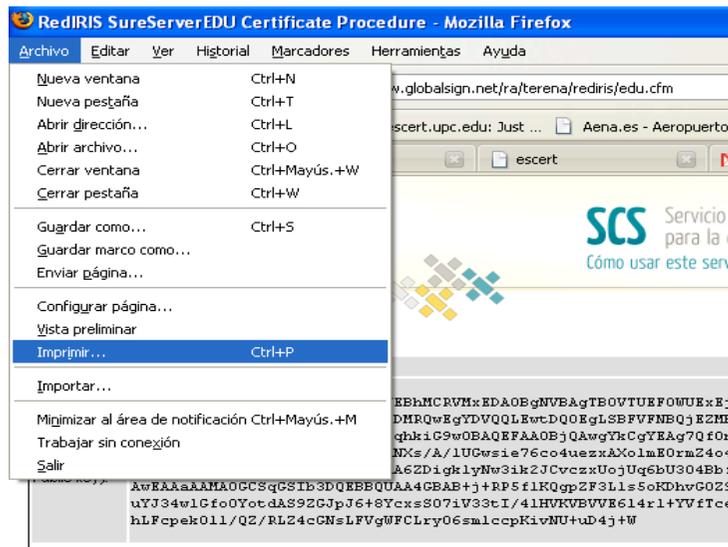


cert@escert.upc.edu

Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas

Aplicación GlobalSign (3/4)

- Verificamos todos los datos
- Imprimimos a PDF la información de la petición a través de CutePDF
 - Guardar como [AAAMMDD.vv][CN] CSR.pdf

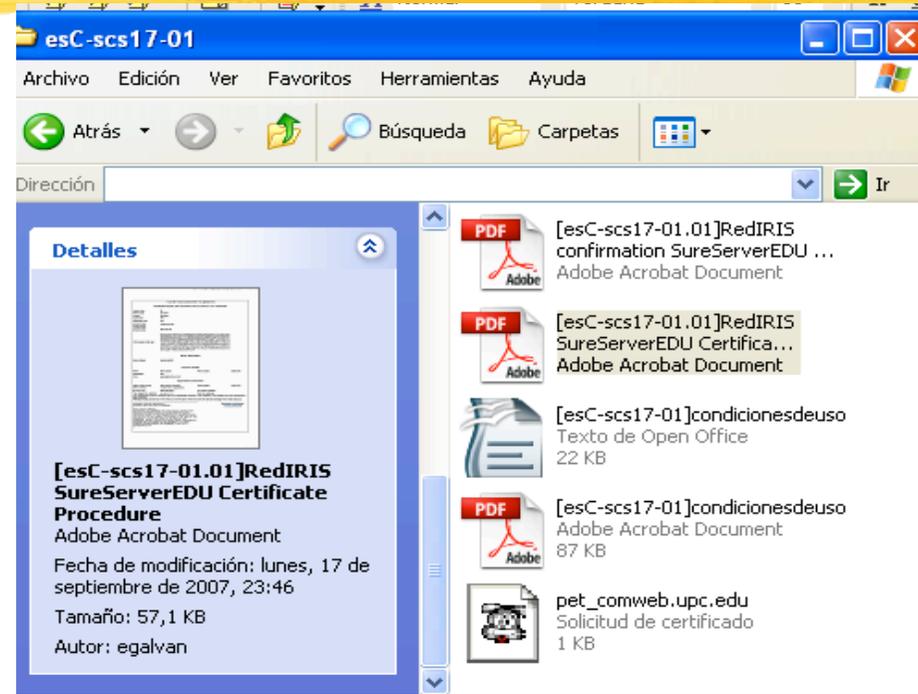


cert@escert.upc.edu

Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas

Aplicación GlobalSign (4/4)

- Verificamos el documento creado
- Clicar en el botón del paso 3



STEP 3: CONFIRM INFORMATION

You are about to send your request to us for processing.

Please check the details below and read the subscriber agreement before clicking the button to request your certificate!

I confirm the information below and wish to proceed with this certificate request!

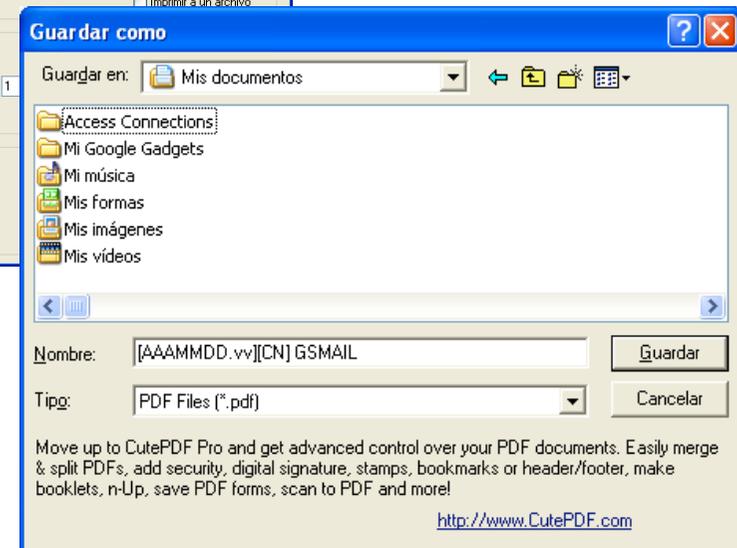
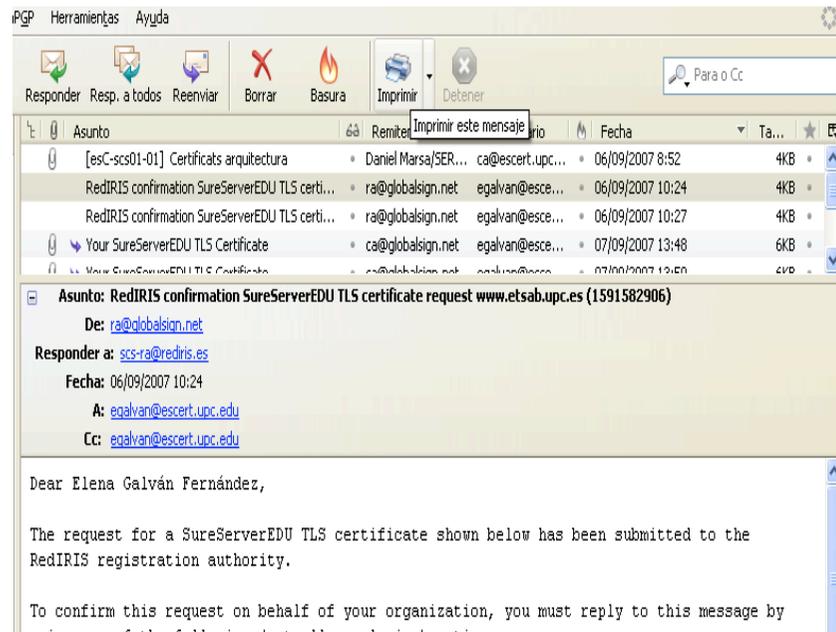


cert@escert.upc.edu

**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**

Correo GlobalSign

- Imprimimos en PDF el correo recibido de GS

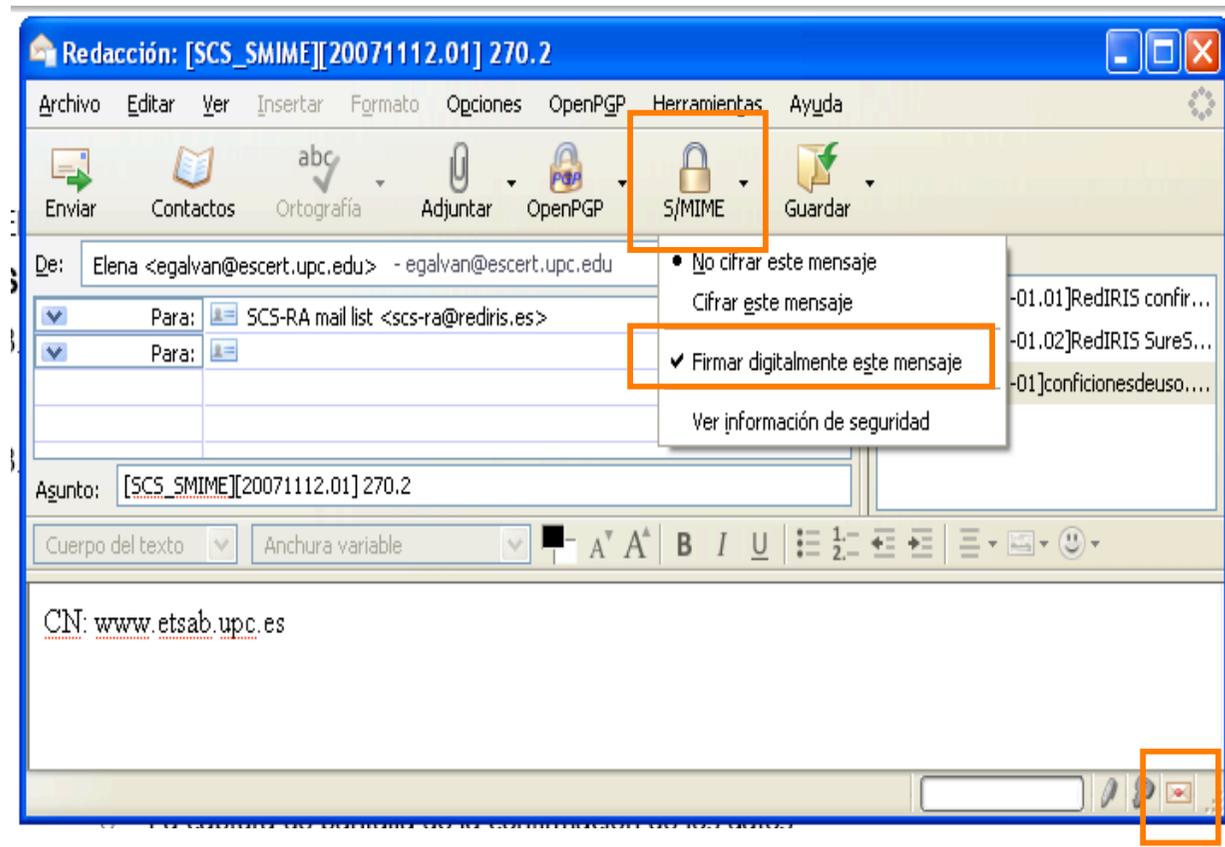


cert@escert.upc.edu

**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**

Correo para scs-ra

- Una vez tenemos todos los PDF's, los incorporamos al correo específico, con el asunto pertinente
- Indicamos en el Thunderbird que se firme utilizando nuestro certificado



Esperamos...

- Ahora falta la respuesta por parte de GS
- Si no llega...
 - Podemos buscar el certificado a ver si se ha emitido y no ha acabado de llegar el correo
 - <http://secure.globalsign.net/phoenixng/services.cfm?id=1413967734&reset=yes>
 - Por CN, por ejemplo



scs-user **Foro de ayuda a los administradores de
servidores que usan certificados SCS**

scs-ra@rediris.es

cert@escert.upc.edu



cert@escert.upc.edu

**Equipo de Seguridad y Coordinación
de Emergencias en Redes Telemáticas**