#### **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

### 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





cert@escert.upc.edu

#### **Nueva Gestión**

Documentación PROXY-SCS Información para los administradores Certificado digital Primera etapa de testeo Problemas de validación Validación y mejor organización Entorno CutePDF



#### 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 sevicio, utilizando para ello cualquier método de identificación electrónico reconocido por la legislación española.

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



cert@escert.upc.edu

#### 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

#### Visor de certificados:"268800e96fb95137b77c4146fda4c3c8\_8d5efedb-99... 💈





cert@escert.upc.edu

#### 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







Equipo de Seguridad y Coordinación de Emergencias en Redes Telemáticas

Aceptar

Seguridad del mensaje

aue se envió.

El mensaie está firmado

Certificado emitido por: EC-IDCat

El mensaje no está cifrado

Firmado por: MARIA-ELENA GALVAN FERNANDEZ

Direcciones de correo electrónico: egalvan@escert.upc.edu

Este mensaje incluye una firma digital válida. El mensaje no ha sido manipulado desde

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.

#### **Problemas de validación**

- Empezaron los envíos de la documentación y llegó un DdCU con unas cuantas peticiones....
- Se envió un correo con muchos adjuntos
- iProblemas 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





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



#### **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

#### 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





cert@escert.upc.edu

## Aplicación GlobalSign (1/4)

	1. Options	
	No. Years:	💿 1 year 🔿 2 years 🔿 3 years
	Type of Server Certificate	Please Select:
	Webserver Type:	Please Select:
2.Cert	ificate Request File (CSR)	
You ca	an do a copy & paste. Open the CSR ir	n a text editor:
1. Loca	ate the section in the file that looks like	
 , ,	-BEGIN CERTIFICATE REQUEST-	
····/	/ -END CERTIFICATE REQUEST	
2. Pas lines).	te it in the input field below (including t	the BEGIN and END- 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 containin the CSR you want to upload. Examinar



#### Aplicación GlobalSign (2/4)

RedIRIS Sur	eServerEDU Certificate Proced	lure - Mozilla	Firefox		- 7 🗙
<u>A</u> rchivo <u>E</u> ditar	⊻er Historial <u>M</u> arcadores Her	ramien <u>t</u> as Ayy	<u>i</u> da		
🦛 • 🧼 •	C 📀 🏠 🗋 https://www	v.globalsign.net/r	ra/terena/rediris/edu.cfm	🖉 🔻 🕨 🔀 Google	Q
🕺 Últimas noticia	as 📄 RedIRIS - Jornadas T 📄 e	scert.upc.edu: J	ust 📄 Aena.es - Aeropuerto 💿 RedIRIS SureSer	rverE 🎎 RedIRIS - Guía Básica 🔯 Introducción a la infor	*
	₽IRIS	<u>.</u>	SCS Servicio de Certificados de S para la comunidad RedIRIS Cómo usar este servicio	iervidor	
This informa	ST Please fill ation will be used to verify ti It will no	EP 2: ENTER out the follo he identity c t be publishe	R INFORMATION wing registration form. of your organization and for administration ed in your certificate.	purposes.	
	Total Cost: SureServ	verEDU TLS em	ailserver - 2 years - 1 licence : 0 EUR		
	Technical Contact		Organisation Information		
Surname:	Galvan	Admin Contact	Elena Galván Fernández		
First Name:	Elena	Person:			
Function:	technical contact	Email:	egalvan@escert.upc.edu		
Organization:	UPC	Organization:	UPC		
Phone number:	934015795	Street & number:	C/Jordi Girona, modul D6-007		
Email:	egalvan@escert.upc.edu	Zip/Post Code (antional):	08034 City: Barcelo	na	
The technical co	ontact is the person who is authorised	Country:	ES		
This may be y appropriate te	namian your secure webserver. our organisation's webmaster or the chnical support staff at your Internet Service Provider (ISP).	Phone number:	934015795 Fax (optional):		
		Trade Register No. (optional):	esC-scs15-03.01 DUIIS IIo. (optional):		
I Terminado					~



## 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

BedIRIS SureServerEDU Certificate Procedure - Mozilla Firefox	Imprimir ?X	Connections				
<u>Archivo</u> Editar Ver Historial Marcadores Herramientas Ayuda	Impresora	Mi Google Gadgets				
Nueva ventana Ctrl+N v.globalsign.net/ra/terena/rediris/edu.cfm	Nombre: CutePDFWriter Propiedades	🚵 Mi música				
Abrir dirección	Tipo: CutePDF Writer	🛗 Mis formas				
Abrir archivo Ctrl+O	Ubicación: CPW2:	📇 Mis imágenes				
Cerrar ventana Ctrl+Mayús.+W 🖾 🗋 escert 💽 💽	Comentario: Imprimir a un archivo	Mis vídeos				
<u>C</u> errar pestaña Ctrl+W	Intervalo de impresión Copias					
Guardar como Ctrl+5	⊙ Iodo Número de copjas: 1 ♀					
Guardar marco como	O Páginas de: 1 a: 1					
Enviar página		Nombre: [AAAMMDD.vv][CN1CSB] Guardar				
Configurar página	Imprimir marcos					
<u>V</u> ista preliminar	O Iguaj que en la pantalla	Tipo: PDF Files (* ndf)  Cancelar				
Imprimir Ctrl+P	El marco seleccionado					
Importar RBhMCRVMx RDAOB aNVBA a TBOVTURFONUE x E1	O Cada marco por separado Aceptar Cancelar	Move up to CutePDF Pro and get advanced control over your PDF documents. Easily merge				
Minimizar al área de notificación Ctrl+Mayús,+M DMRQwEgYDVQQLEwtDQ0EgLSBFVFNBQjEZMB		a split FDF's, add security, digital signature, stamps, bookmarks of neader/tooter, make booklets, p.U.p. save PDE forms, scan to PDE and morel				
Trabajar sin conexión qhkiG9w0BAQEFAA0BjQAwgYkCgYEAg7Qf0n NXs/A/1UCwsie76co4uezxAXo1mE0rm24o4		bookieks, mop, saver of forms, scanker of and more:				
Salir A62DigklyNw3ik2JCvczxUojUq6bU304Bbf		http://www.CutePDF.com				
AwEAAAAMAOGCSqGSIb3DQEBEQUAA4GBAB+j+RP5f1KQgp2F3L1s5oKDhvG029 uYJ34w1Gfo0YotdAS92GJpJ6+8YcxsS07iV33t1/41HVKVBVVE614r1+YVfTce						
hLFcpek011/Q2/RLZ4cGNsLFVgWFCLry06smlccpKivNU+uD4j+W						

Guardar como

Currenter and



Equipo de Seguridad y Coordinación de Emergencias en Redes Telemáticas ? X

## 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

#### **Correo GlobalSign**

#### Imprimimos en PDF el correo recibido de GS

P Herramien <u>t</u> as Ayuda				0
Responder Resp. a todos Reenviar Borrar Bas	ura Imprimir Detener	Para o Cc		
ት 🕖 🛛 Asunto	6à Remiter Imprimir este mensaje rio	🗄 Fecha 🔹	Ta  ★	₽,
[esC-scs01-01] Certificats arquitectura	<ul> <li>Daniel Marsa/SER ca@escert.upc</li> </ul>	<ul> <li>06/09/2007 8:52</li> </ul>	4KB •	^
RedIRIS confirmation SureServerEDU TLS certi.	• ra@globalsign.net egalvan@esce	<ul> <li>06/09/2007 10:24</li> </ul>	4KB •	
RedIRIS confirmation SureServerEDU TLS certi.	• ra@globalsign.net egalvan@esce	<ul> <li>06/09/2007 10:27</li> </ul>	4KB •	-
🅘 👒 Your SureServerEDU TLS Certificate	<ul> <li>ca@globalsign.net egalvan@esce</li> </ul>	<ul> <li>07/09/2007 13:48</li> </ul>	6KB •	
A Vour GuroContovEDULTI C CovERcoto	- co@alabalcian.pot _ agaluan@acco	- 07/00/2007 12/50	۲۷D .	*
De: ra@olobalsion.net Responder a: scs-ra@redris.es Fecha: 06/09/2007 10:24 A: eggavan@escert.upc.edu Cc: eggavan@escert.upc.edu				
Dear Elena Galván Fernández, The request for a SureServerEDU TLS RedIRIS registration authority.	certificate shown below has	been submitted to the		^

To confirm this request on behalf of your organization, you must reply to this message by





#### 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

🖨 R	edacción: [S	SCS_	SMIME][200711	2.01] 270	).2				
<u>A</u> rchi	ivo <u>E</u> ditar	<u>V</u> er	Insertar Formato	Opciones	OpenP <u>G</u> P	Herramientas	Ay <u>u</u> da		0
Envi	iar Conta	] ctos	abç Ortografía	U - Adjuntar		S/MIME -	Guardar		
<u>D</u> e:	Elena <egalv< th=""><th>an@e</th><th>escert.upc.edu&gt; -e</th><th>galvan@esce</th><th>rt.upc.edu</th><th>• <u>N</u>o cifrar</th><th>este mensaje</th><th></th><th></th></egalv<>	an@e	escert.upc.edu> -e	galvan@esce	rt.upc.edu	• <u>N</u> o cifrar	este mensaje		
	Para:	<u>2</u> =	SCS-RA mail list <scs< th=""><th>-ra@rediris.e</th><th>s&gt;</th><th>Cifrar <u>e</u>st</th><th>e mensaje</th><th></th><th>-01.01]RedIRIS confir</th></scs<>	-ra@rediris.e	s>	Cifrar <u>e</u> st	e mensaje		-01.01]RedIRIS confir
	Para:	2=				✓ Firmar die	italmente este i	mensaie	-01.02]RedIRIS SureS
						- Timarai	gicalino neo 0 <u>2</u> co 1	monodjo	-01]conficionesdeuso
						Ver inforr	mación de segur	idad	
A <u>s</u> uni	to: [SCS_SM	[ME]	20071112.01]270.2						
Cue	Cuerpo del texto       Anchura variable $\checkmark$ $\blacksquare$								
<u>CN: www.etsab.upc.</u> es									





- 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=y
    es
    - 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