MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

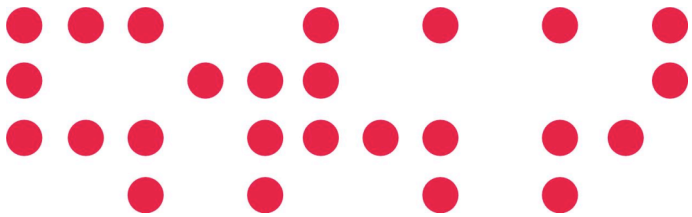
SCS: servicio de certificados de servidor

Daniel García - Javi Masa

26 junio 2007 - gt2007 - Madrid

RedIRIS

Índice



- Números del servicio
  - Identidades digitales certificada: 933
  - Certificados emitidos: 687
    - Validos: 665
    - Expirados: 8
    - Revocados 22

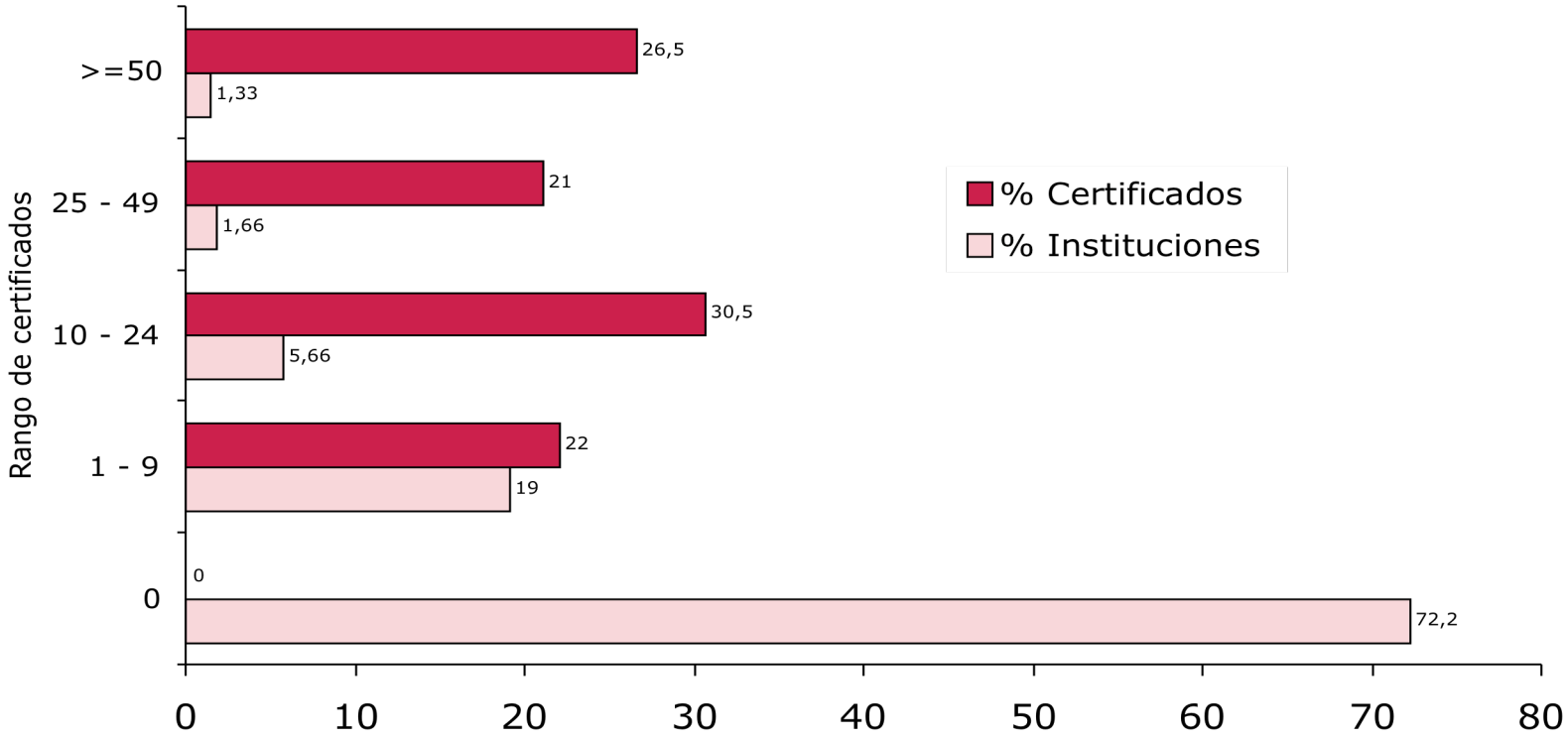
Actualidad - Estadísticas

- Más de 50
  - 76 uc3m.es
  - 70 upv.es
  - 50 url.edu
  - 50 ulpgc.es
- 49 a 25
  - 47 uam.es
  - 44 csic.es
  - 39 uvigo.es
  - 37 uma.es
  - 29 upf.edu
- 24 a 10
  - 24 uclm.es
  - 23 cica.es
  - 21 unirioja.es, cesga.es
  - 19 usc.es, upm.es
  - 17 uib.es, uco.es
  - 15 unizar.es, rediris.es, icfo.es
  - 14 unileon.es, udc.es, uah.es, bsc.es
  - 13 ucm.es
  - 10 urjc.es
- Menos de 10
  - 9 cert 2 inst
  - 8 cert 6 inst
  - 7 cert 1 inst
  - 6 cert 1 inst
  - 5 cert 6 inst
  - 4 cert 3 inst
  - 3 cert 6 inst
  - 2 cert 6 inst
  - 1 cert 18 inst

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Distribución de certificados por instituciones

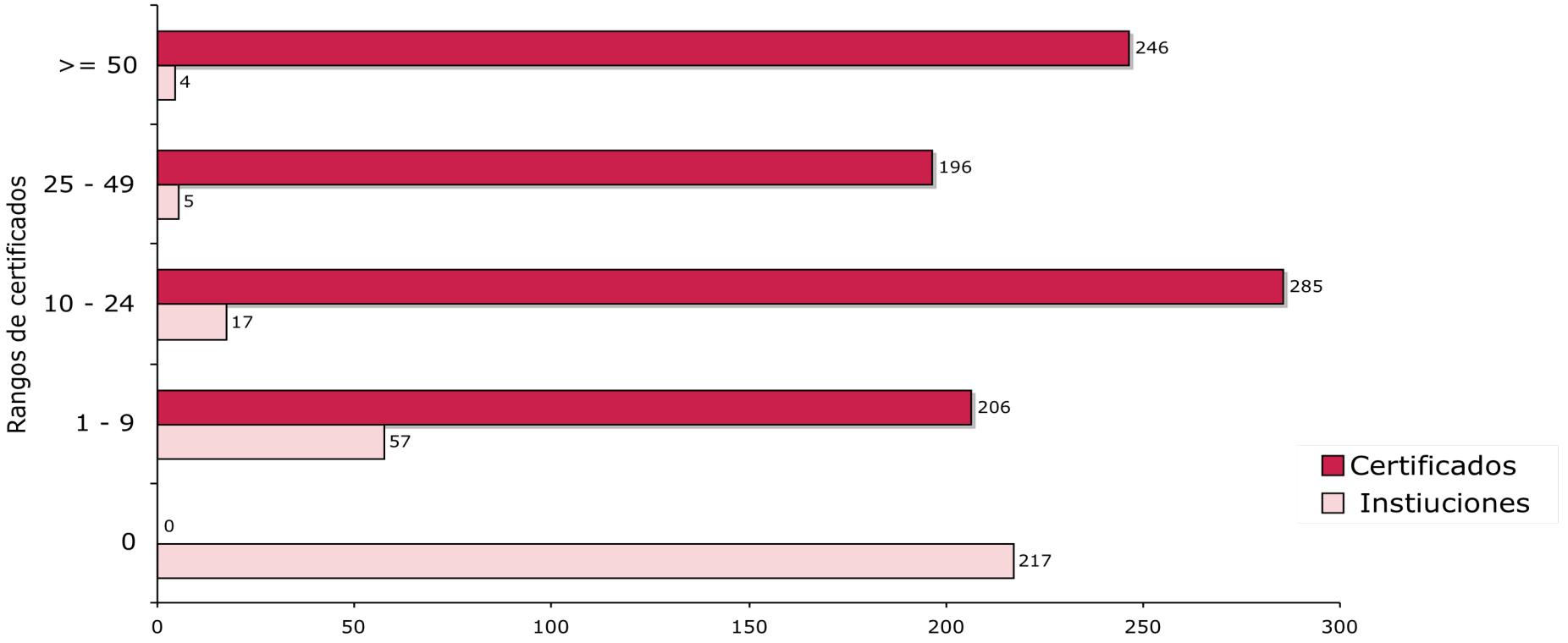


Red IRIS

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

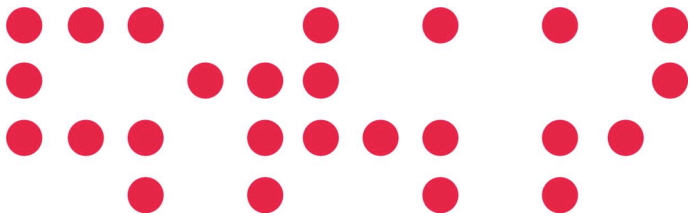
red.es

Distribucion de certificados por instituciones



Red IRIS

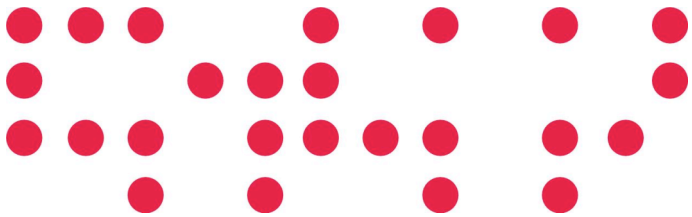
Índice



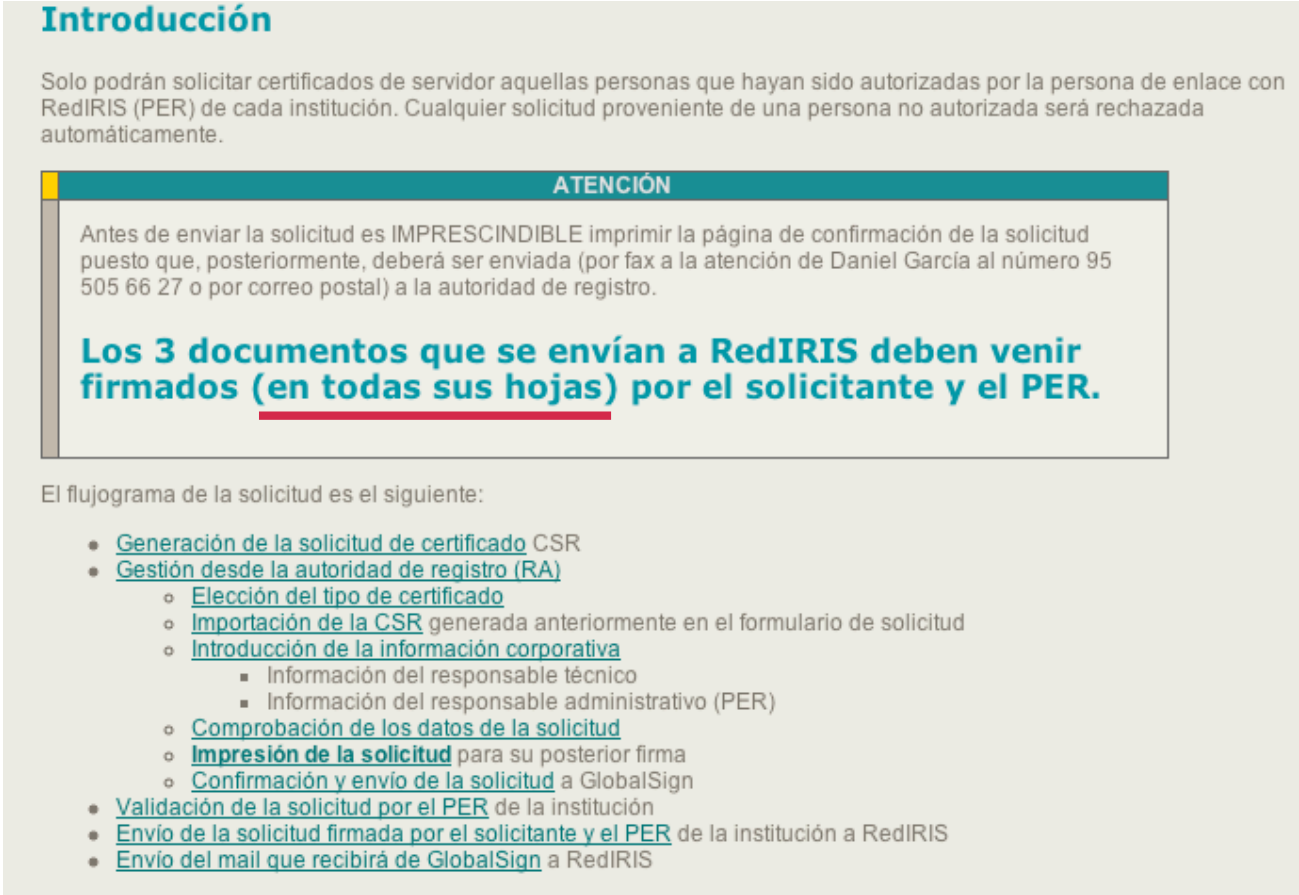
Errores Comunes

- Faltan las Firmas del PER o del solicitante
  - Ya sea en una o en todas las caras de las hojas
- No se han firmado todas las caras de todas las hojas
- Errores en los dominios
  - Prevalidarlos
  - No es el titular
- Falta documentación ó mal cumplimentada
- Faltan caras de las hojas en los faxes recibidos

Índice



- Acceso a la guía básica de solicitud de SCS
  - http://www.rediris.es/pki/scs/doc/userguide.es.html



Introducción

Solo podrán solicitar certificados de servidor aquellas personas que hayan sido autorizadas por la persona de enlace con RedIRIS (PER) de cada institución. Cualquier solicitud proveniente de una persona no autorizada será rechazada automáticamente.

ATENCIÓN

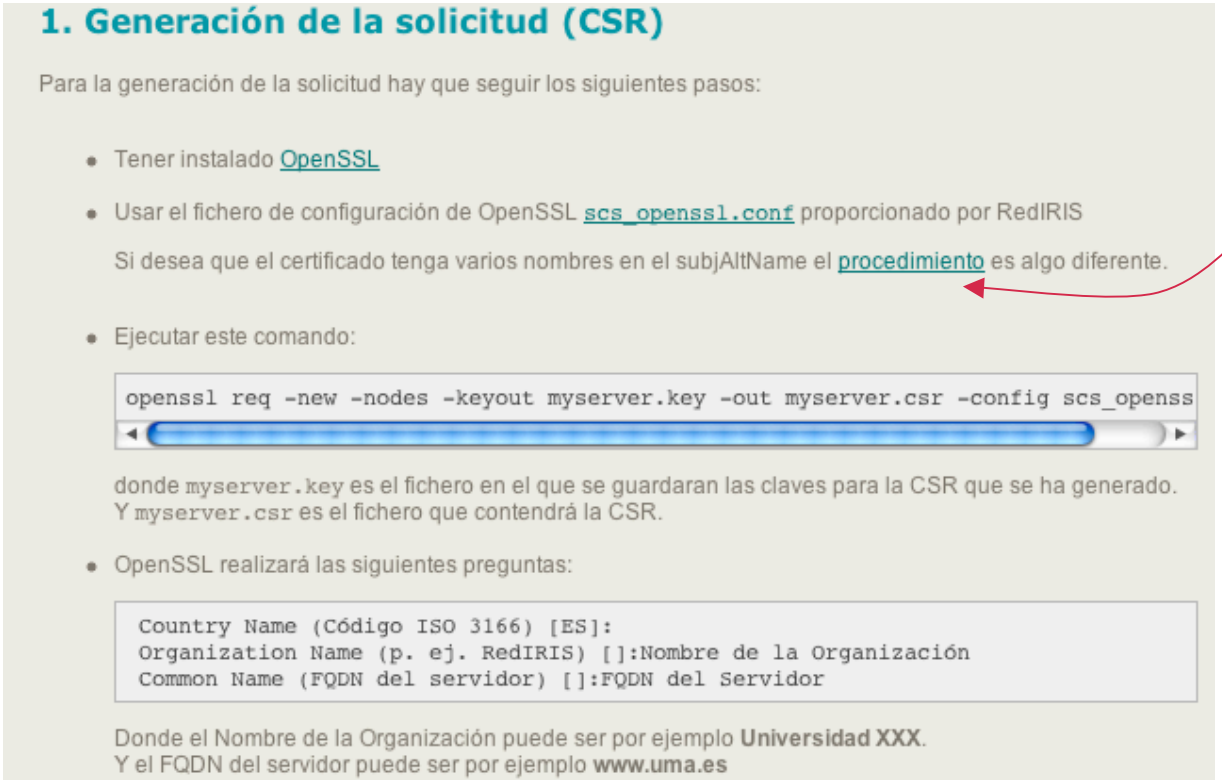
Antes de enviar la solicitud es IMPRESCINDIBLE imprimir la página de confirmación de la solicitud puesto que, posteriormente, deberá ser enviada (por fax a la atención de Daniel García al número 95 505 66 27 o por correo postal) a la autoridad de registro.

Los 3 documentos que se envían a RedIRIS deben venir firmados (en todas sus hojas) por el solicitante y el PER.

El flujograma de la solicitud es el siguiente:

- Generación de la solicitud de certificado CSR
- Gestión desde la autoridad de registro (RA)
  - Elección del tipo de certificado
  - Importación de la CSR generada anteriormente en el formulario de solicitud
  - Introducción de la información corporativa
    - Información del responsable técnico
    - Información del responsable administrativo (PER)
  - Comprobación de los datos de la solicitud
  - **Impresión de la solicitud** para su posterior firma
  - Confirmación y envío de la solicitud a GlobalSign
- Validación de la solicitud por el PER de la institución
- Envío de la solicitud firmada por el solicitante y el PER de la institución a RedIRIS
- Envío del mail que recibirá de GlobalSign a RedIRIS

- Generación de la CSR



1. Generación de la solicitud (CSR)

Para la generación de la solicitud hay que seguir los siguientes pasos:

- Tener instalado OpenSSL
- Usar el fichero de configuración de OpenSSL `scs_openssl.conf` proporcionado por RedIRIS

  Si desea que el certificado tenga varios nombres en el subjAltName el procedimiento es algo diferente.

- Ejecutar este comando:

```
openssl req -new -nodes -keyout myserver.key -out myserver.csr -config scs_openss
```

  donde `myserver.key` es el fichero en el que se guardaran las claves para la CSR que se ha generado.
  Y `myserver.csr` es el fichero que contendrá la CSR.

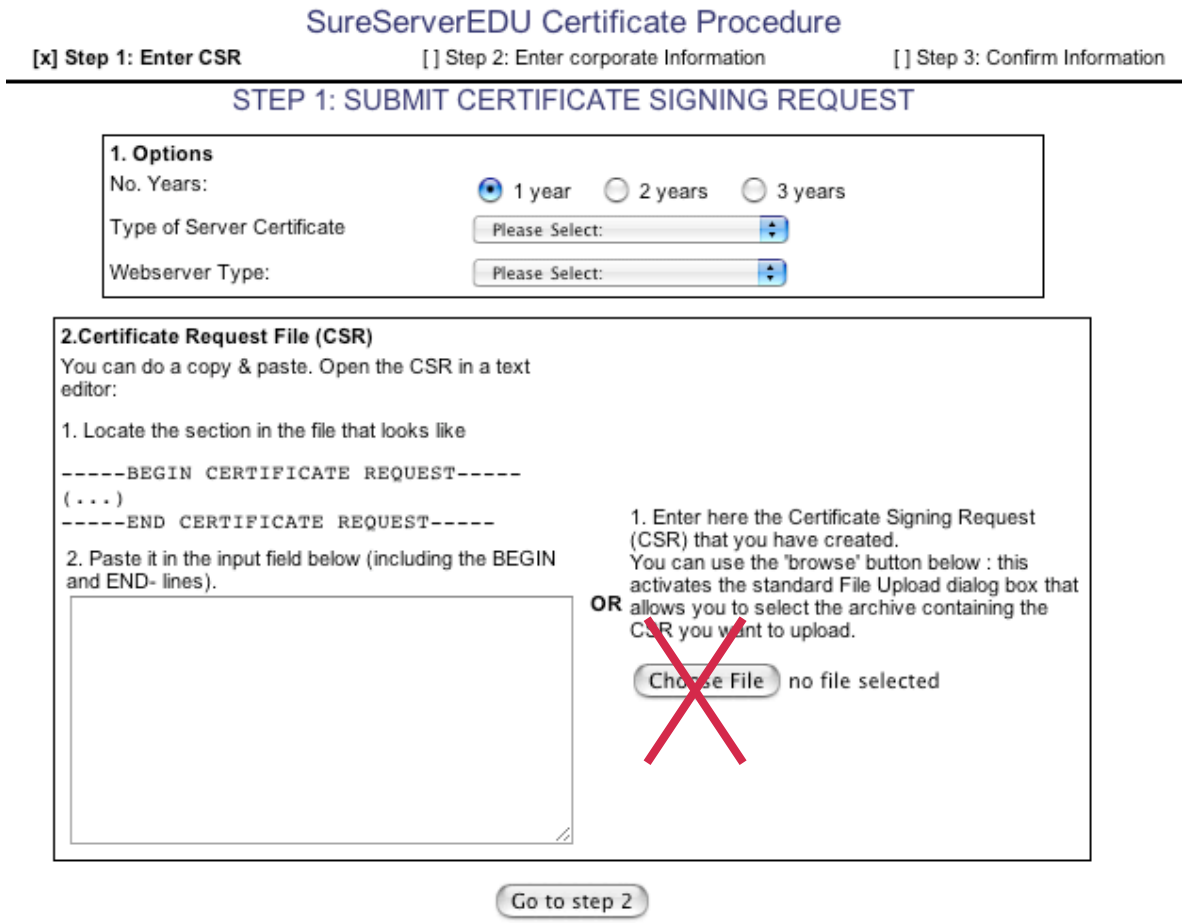
- OpenSSL realizará las siguientes preguntas:

```
Country Name (Código ISO 3166) [ES]:
Organization Name (p. ej. RedIRIS) []:Nombre de la Organización
Common Name (FQDN del servidor) []:FQDN del Servidor
```

  Donde el Nombre de la Organización puede ser por ejemplo **Universidad XXX**.
  Y el FQDN del servidor puede ser por ejemplo **www.uma.es**

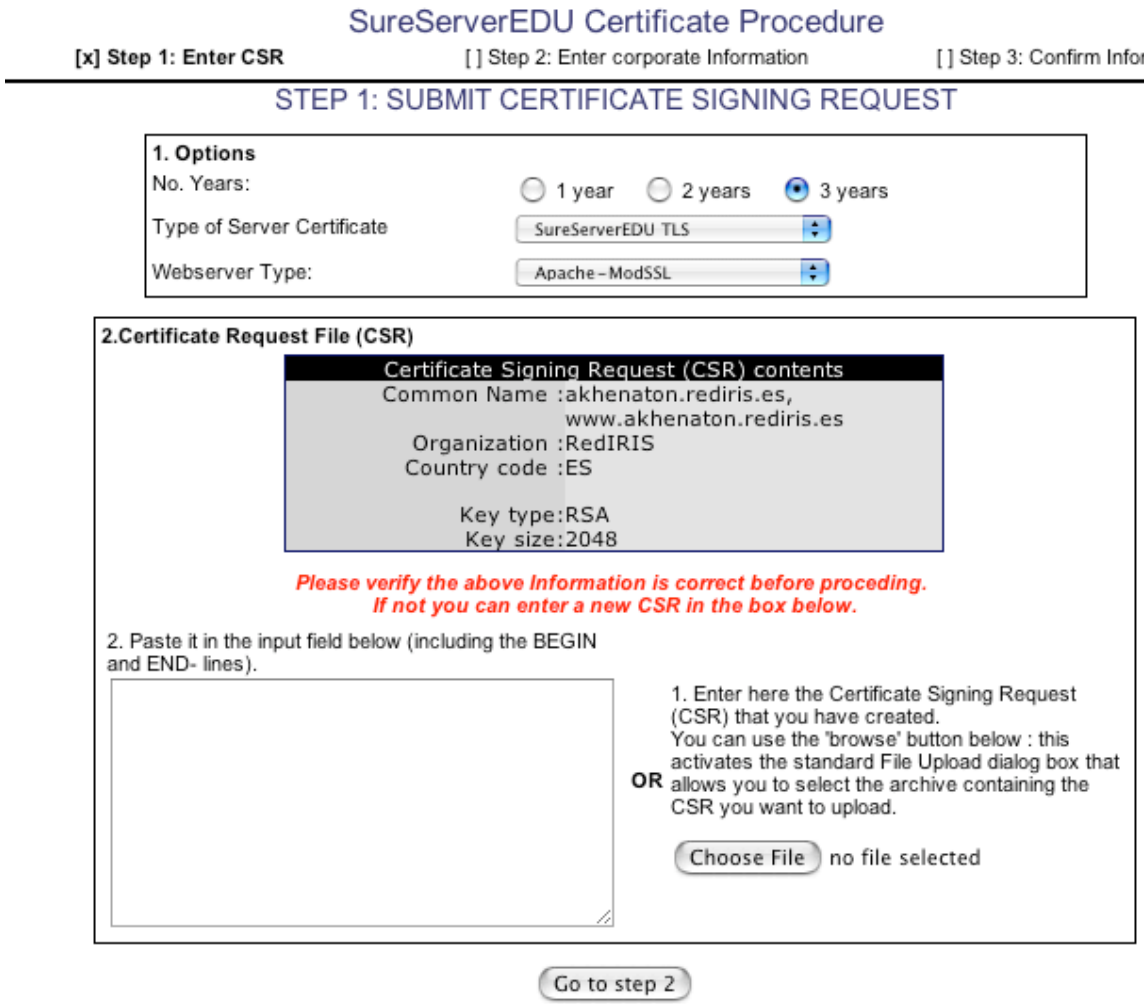
- Editar el fichero de configuración de openssl
- Se pueden definir SubjectAltNames
- Se generan dos ficheros, CSR y privKey

Envío de la CSR I



- Elegimos el tiempo de vida del certificado
- El perfil del certificado
  - **SureServerEDU TLS**
  - SureServerEDU TLS emailserver
  - SureServerEDU
- El tipo del servidor que albergará el certificado
- Pegamos la CSR
  - No usamos ‘browser button’

Envío de la CSR II

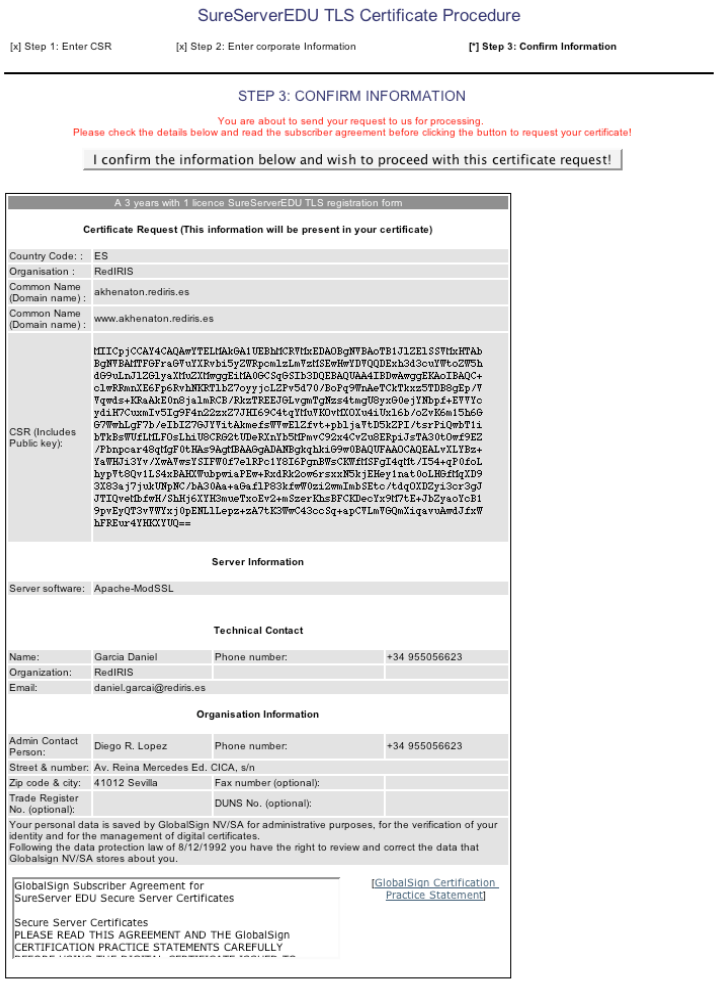


- Confirmamos los datos de la CSR

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Envío de la CSR III



SureServerEDU TLS Certificate Procedure

[x] Step 1: Enter CSR [x] Step 2: Enter corporate Information [*] Step 3: Confirm Information

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!

A 3 years with 1 licence SureServerEDU TLS registration form

Certificate Request (This information will be present in your certificate)

Country Code: :	ES
Organisation :	RedIRIS
Common Name (Domain name) :	akhenaton.rediris.es
Common Name (Domain name) :	www.akhenaton.rediris.es
CSR (Includes Public key):	MIICpjCCAY4CAQAwTELMAkGA1UEBhMCRVMxEDAOBgNVBAoTB1JlZElSUzExMTAb BgNVBAMTFGFra6YuYXRvbi5yZWRpcmlzLmVzMSEwHwYDTQQDExh3d3cuYWtoZW5h d69uLnJlZGlyaXRoZXMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+ clwRRwnXE6Fp6RvhNKRTlbZ7oyyjcLZFv5d70/BoFq9FnAeTCkTkxz5TDB8gEp/Y YqwdsKRaAkE0n8jalmRCB/RkzTKEEJGLvgwTgNzs4tmgU8yx60ejYNbpf+EVYc ydiH7CuxmIv5Ig9F4nZ2rxZ7JKI69C4tgYHbVKOwtUOIx4iUnl6b/oZvK6m15h669 G7WehLgF7b/eIbIZ7GJYYitAkmefsWYwElZfvt+pbljaYtD5k2PI/tsrPiQwbTli bTkBsWUfLMLF0sLhiU8CRG2tUDeRXnYb5tPmvC92x4CvZu8ERpiJsTA30tOwf9EZ /Pbnpcar48qfgF0tHAs9AqtBAA8gADANBgkqhki69w0BAQUFAAOCAQEALvXLYBz+ YaWHJi3Yv/XwAYwsYSIFW0f7elRPc1Y8I6PgnBWsCKWfHfSFgI4qtt/I54+qP0foL hypYt8Qv1LS4xBAHUWubwiaPEw+RxdRk2ow6rsxxN5kjEHey1nat0oLH6ftqXD9 3X83aj7jukUNpNC/bA30Aa+aGaflP83kfeW0zi2wmImbSEto/tdqOXDZyi3cr3gJ JTIQvetDfwH/ShHj6XYH3wueTxoEv2+mSzerKbsBFCKDecYx9H7tE+JbZyaoYoB1 9prEyQT3vYWYxjOpENL1Lepz+zA7tK3WwC43ccSq+apCTLaVGQmXiqavoAmdJfxW hFPEur4YHXXYUQ==

Server Information

Server software:	Apache-ModSSL

Technical Contact

Name:	Garcia Daniel	Phone number:	+34 955056623
Organization:	RedIRIS		
Email:	daniel.garcai@rediris.es		

Organisation Information

Admin Contact Person:	Diego R. Lopez	Phone number:	+34 955056623
Street & number:	Av. Reina Mercedes Ed. CICA, s/n		
Zip code & city:	41012 Sevilla	Fax number (optional):	
Trade Register No. (optional):		DUNS No. (optional):	

Your personal data is saved by GlobalSign NV/SA for administrative purposes, for the verification of your identity and for the management of digital certificates.
Following the data protection law of 8/12/1992 you have the right to review and correct the data that GlobalsIgn NV/SA stores about you.

GlobalSign Subscriber Agreement for
SureServer EDU Secure Server Certificates

Secure Server Certificates
PLEASE READ THIS AGREEMENT AND THE GlobalSign
CERTIFICATION PRACTICE STATEMENTS CAREFULLY

[GlobalSign Certification Practice Statement]

- Capturamos esta página o la imprimimos
- Confirmamos de nuevo los datos de la CSR
  - La firmamos
  - en todas sus caras :-)

Red IRIS

Demo

- Mail de GlobalSign
  - Capturamos o imprimimos el correo de confirmación de GlobalSign
  - Firmamos la copia impresa
    - En todas sus caras

De: ra@globalsign.net
Asunto: **RedIRIS confirmation SureServerEDU TLS certificate request akhenaton.rediris.es,www.akhenaton.rediris.es (1916308087)**
Para: Diego R. López
Cc: Daniel García Franco
Responder a: SCS-RA mail list

Dear Diego R. Lopez,

The request for a SureServerEDU TLS certificate shown below has been submitted to the RedIRIS registration authority.

To confirm this request on behalf of your organization, you must reply to this message by using one of the following (mutually exclusive) options:

1) print this e-mail message, sign it by hand and return to us by either:

a) postal mail,
b) fax,
c) e-mail, where the scanned message is attached as a PDF document (or similar);

2) reply to this message with a digitally signed e-mail. The certificate used for signing must reflect an adequate assurance level; when considering this option for the first time please contact us to determine whether your (personal) certificate qualifies for this purpose.

By replying to this message, you confirm that the person listed as the technical contact is entitled to request a certificate as shown below and agrees to be bound by the terms of the subscriber agreement available at http://www.globalsign.net/repository.

The certificate will be issued after a successful verification of your reply, which usually happens within one to three business days. You will receive a follow up email when your certificate is ready.

Note: if you do not reply to this message within 15 days, we will cancel this request without further notice.

RedIRIS Registration authority
Entidad Pública Empresarial Red.es,
Edificio Bronce,
Plaza Manuel Gómez Moreno, s/n 28020 Madrid
fax: +34 955 056 627 www.rediris.es

Details of request order 1916308087, SureServerEDU TLS certificate:

Certificate type	SureServerEDU TLS 1 year
Subject	C=ES, O=RedIRIS, CN=akhenaton.rediris.es, CN=www.akhenaton.rediris.es
CSR	

MIICpjCCAY4CAQAwYTELMAkGA1UEBhMCRVMxEDAOBgNVBAoTB1JlZElSSVMxHTAb
BgNVBAMTFGFraGVuYXRvbi5yZWRpcmlzLmVzMSEwHwYDVQQDExh3d3cuYWtoZW5h
dG9uLnJlZGlyaXMuZXMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+
ciwRRmnXE6Fp6RvhNKRTlbZ7oyyjcLZPv5d70/BoPq9WmAeTCkTkxz5TDB8gEp/V
Vqwds+kRaAkE0n8jalmRCB/RkzTREJGLvgmTgNzs4tmgU8yxG0ejYNbpf+EVYYc
ydiH7CuxmIv5Ig9F4n2ZzxZ7JHI69C4tqYMuVKOvMtXXu4iUxi6b/oZvKGm15h6G
G7WwhLgF7b/eIbIZ7GJVitAkmefsWVvEiZfvt+pbljaVtD5kZPI/tsrPiQvbT1i
bTkBs9UfLMLFOsLhiU8CRG2tUDeRXnYb5MPwvC92x4CvZuBERpiJsTA30t0wf9EZ
/PbnpcarI8qMgF8tHAs9AgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEALvXLYBz+
YaWHJi3Yv/XwAVwsYSIFW0f7elRPc1Y8I6PgnB9sCKWfMSFgI4qMt/I54+qP0foL
hypVt8Qv1LS4xBAHXYubpwiaPEw+RxdRk2ow6rsxxN5kjEHey1natBoLHGfMqXD9
3X83qj7jukUNpNC/bA30Aa+aGafiP83kfwW0zi2vmImbSEtc/tdqOXDZyi3cr3gJ
JTIQveMbfvH/ShHj6XYH3aueTxoEv2+mSzerKhsBFCKDecYx9M7tE+JbZyaoYcB1
9pvEyQT3vVWYxj0pENLlLepz+zA7tK3WwC43ccSq+apCVLmVGQmXiqavuAwdJfxW
hFREur4YHKXYUQ==

Server software	Apache-ModSSL

Technical contact

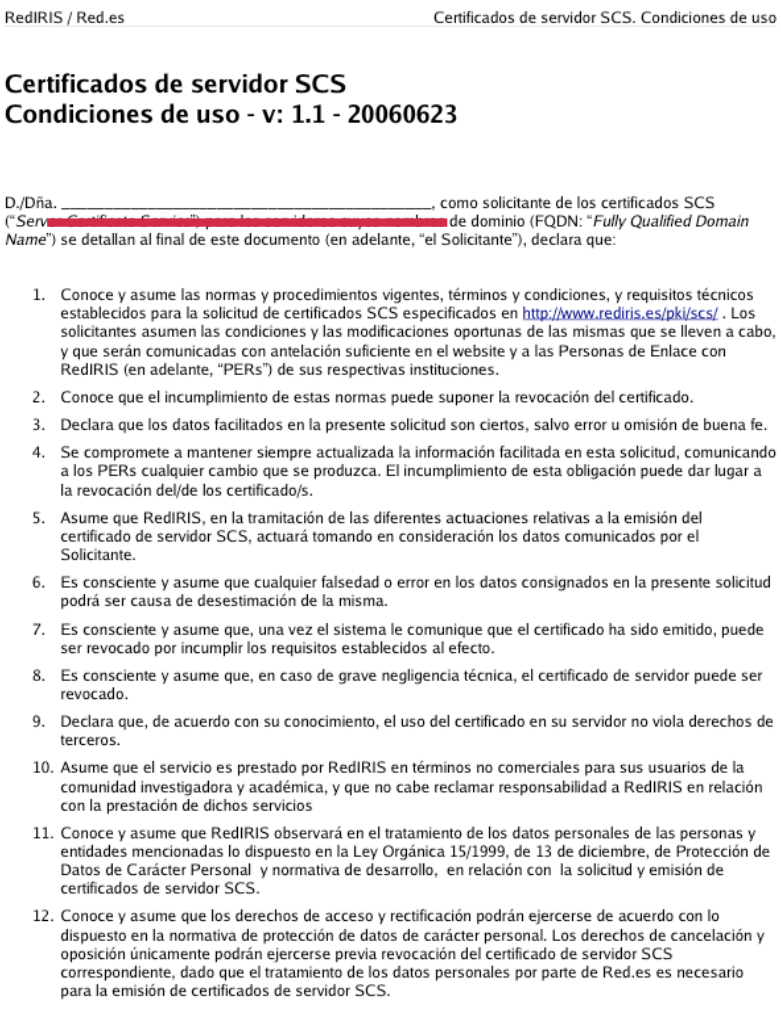
Name	Garcia Daniel
Organization	RedIRIS
E-Mail	daniel.garcia@rediris.es
Phone number	+34 955056623

Admin contact

Name	Diego R. Lopez
Organization	RedIRIS
Street address	Av Reina Mercedes Ed. CICA, s/n
Zip code, city	41012 Sevilla
E-Mail	diego.lopez@rediris.es
Phone number	+34 955056623
Fax number	
Trade register no.	

Demo

- Doc. condiciones de uso 1/2
  - Leemos detalladamente el documento
  - Rellenamos el nombre del solicitante
    - Es el responsable técnico



RedIRIS / Red.es — Certificados de servidor SCS. Condiciones de uso

Certificados de servidor SCS
Condiciones de uso - v: 1.1 - 20060623

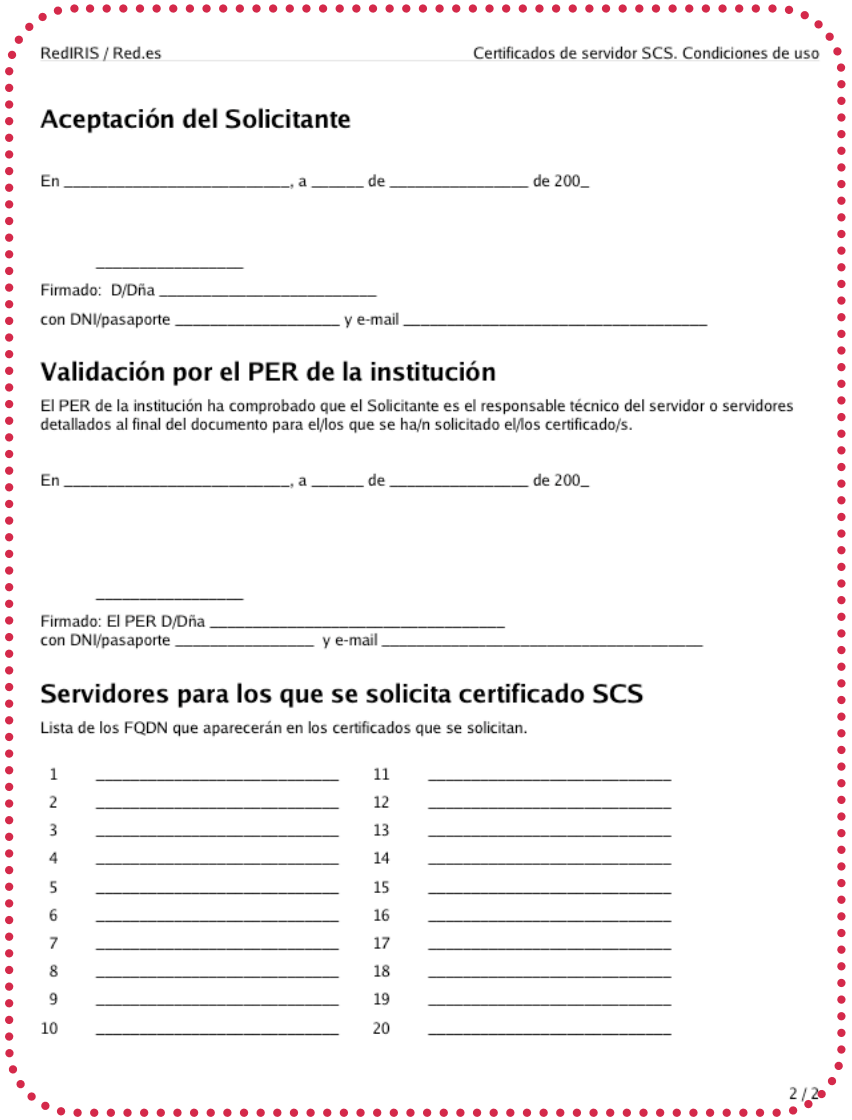
D./Dña. _____, como solicitante de los certificados SCS ("*Serv[redacted]*de dominio (FQDN: "*Fully Qualified Domain Name*") se detallan al final de este documento (en adelante, "el Solicitante"), declara que:

1. Conoce y asume las normas y procedimientos vigentes, términos y condiciones, y requisitos técnicos establecidos para la solicitud de certificados SCS especificados en http://www.rediris.es/pki/scs/ . Los solicitantes asumen las condiciones y las modificaciones oportunas de las mismas que se lleven a cabo, y que serán comunicadas con antelación suficiente en el website y a las Personas de Enlace con RedIRIS (en adelante, "PERs") de sus respectivas instituciones.
2. Conoce que el incumplimiento de estas normas puede suponer la revocación del certificado.
3. Declara que los datos facilitados en la presente solicitud son ciertos, salvo error u omisión de buena fe.
4. Se compromete a mantener siempre actualizada la información facilitada en esta solicitud, comunicando a los PERs cualquier cambio que se produzca. El incumplimiento de esta obligación puede dar lugar a la revocación del/de los certificado/s.
5. Asume que RedIRIS, en la tramitación de las diferentes actuaciones relativas a la emisión del certificado de servidor SCS, actuará tomando en consideración los datos comunicados por el Solicitante.
6. Es consciente y asume que cualquier falsedad o error en los datos consignados en la presente solicitud podrá ser causa de desestimación de la misma.
7. Es consciente y asume que, una vez el sistema le comunique que el certificado ha sido emitido, puede ser revocado por incumplir los requisitos establecidos al efecto.
8. Es consciente y asume que, en caso de grave negligencia técnica, el certificado de servidor puede ser revocado.
9. Declara que, de acuerdo con su conocimiento, el uso del certificado en su servidor no viola derechos de terceros.
10. Asume que el servicio es prestado por RedIRIS en términos no comerciales para sus usuarios de la comunidad investigadora y académica, y que no cabe reclamar responsabilidad a RedIRIS en relación con la prestación de dichos servicios
11. Conoce y asume que RedIRIS observará en el tratamiento de los datos personales de las personas y entidades mencionadas lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, en relación con la solicitud y emisión de certificados de servidor SCS.
12. Conoce y asume que los derechos de acceso y rectificación podrán ejercerse de acuerdo con lo dispuesto en la normativa de protección de datos de carácter personal. Los derechos de cancelación y oposición únicamente podrán ejercerse previa revocación del certificado de servidor SCS correspondiente, dado que el tratamiento de los datos personales por parte de Red.es es necesario para la emisión de certificados de servidor SCS.

1 / 2

Demo

- Doc. condiciones de uso 2/2
  - El solicitante rellena sus datos y firma
  - Rellenamos los datos del PER y pedimos a éste que nos firme
  - En la lista de FQDNs se ponen **todos** los FQDNs para los que se solicitan certificados
    - akhenaton.rediris.es
    - www.akhenaton.rediris.es
  - Un solo Doc de cond. De Uso sirve para más de un certificado
    - Tantos como quepan en la lista de FQDNs



RedIRIS / Red.es Certificados de servidor SCS. Condiciones de uso

Aceptación del Solicitante

En _____, a _____ de _____ de 200_

_____

Firmado: D/Dña _____

con DNI/pasaporte _____ y e-mail _____

Validación por el PER de la institución

El PER de la institución ha comprobado que el Solicitante es el responsable técnico del servidor o servidores detallados al final del documento para el/los que se ha/n solicitado el/los certificado/s.

En _____, a _____ de _____ de 200_

_____

Firmado: El PER D/Dña _____

con DNI/pasaporte _____ y e-mail _____

Servidores para los que se solicita certificado SCS

Lista de los FQDN que aparecerán en los certificados que se solicitan.

1	_____	11	_____
2	_____	12	_____
3	_____	13	_____
4	_____	14	_____
5	_____	15	_____
6	_____	16	_____
7	_____	17	_____
8	_____	18	_____
9	_____	19	_____
10	_____	20	_____

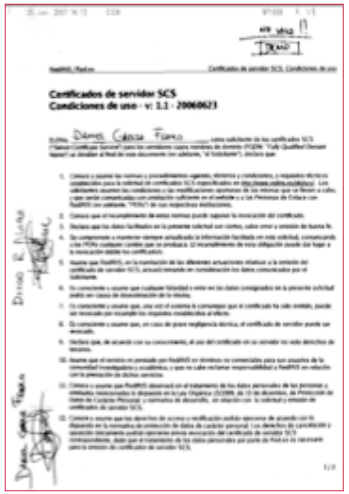
2 / 2

Demo

- Envío por FAX
  - Enviamos toda la documentación al nº de FAX:

    955056623

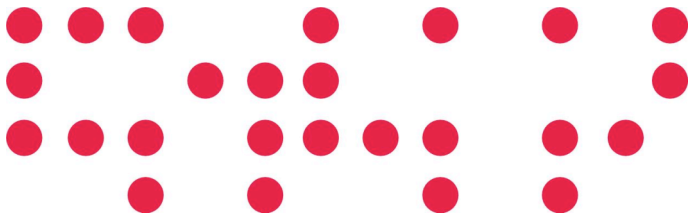
  - A la atención de Daniel García
    - Doc. Cond. de Uso



- CSR

- GSMAIL

Índice



Usos de SCS

- El propósito es crear un canal seguro…
  - No sólo para web, si no también para
    - Radius
    - Ldap
    - Correo
- SCS & Mail
- SCS & Grid
- ¿Certificados personales?
- Ámbito de los certificados SCS

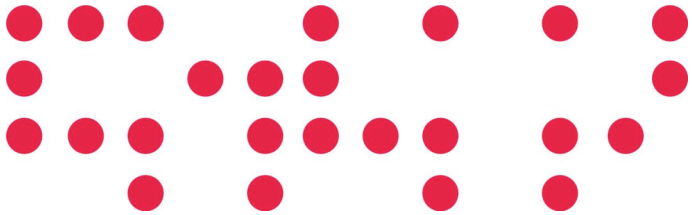
- SCS & Servidores de Correo
  - Firma de correo para evitar la suplantación de servidores
    - Se firma con la identidad del servidor de correo
    - Es la identidad digital certificada

- SCS en Grid
  - Recientemente en la EUGridPMA se ha propuesto un perfil basado en certificados de SCS
  - El perfil es aún un borrador

- Certificados personales para proyectos de e-Ciencia
  - SCS sólo para servidores
  - ¿Y para personas?
    - Podemos usar la pkIRISGrid
    - www.irisgrid.es/pki
    - Con esto podremos firmar y/o cifrar correo con S/MIME

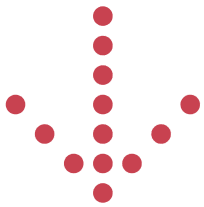
- Ambito de los certificados SCS
  - Hasta ahora sólo en los centro de informática
  - No llegan a los departamentos, sólo a los servidores institucionales
  - Los certificados los puede solicitar cualquiera que pertenezca a la comunidad
    - Servidores de departamentos
    - Servidores de centros
    - Etc

Índice

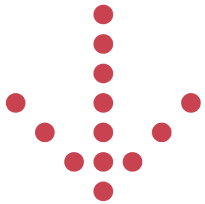


Mejoras en el Proc. De Solicitud

- Piloto con la Universidad Carlos III de Madrid
  - El PER delega en una o varias personas
    - Sólo para el servicio SCS
  - Se envía la documentación por e-mail + S/MIME
- Todo esto nos lo va a aclarar Juan Manuel Canelada



Mejoras en el Proc. De Solicitud



- Las pruebas ha sido satisfactorias
  - Pero aún tenemos que pulir el nuevo procedimiento
    - El problema del solicitante
      - Firma físicamente solicitante + digitalización + firma digital PER
      - Firma digital solicitante + firma digital PER
  - Publicar plantilla del documento de delegación del PER
  - Uso de certificados de la FNMT

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es

Edificio CICA
Avenida Reina Mercedes s/n
41012 Sevilla. España

Tel.: 955 05 66
Fax: 955 05 66
www.red.es

Red IRIS