



**Barcelona
Supercomputing
Center**

Centro Nacional de Supercomputación

BSC-CNS pkIRISGrid User Manual

Version: 1.6

Barcelona, 10. Dec. 2010

Table of Contents

1 Introduction.....	4
1.1 BSC-CNS RA Policy Restrictions.....	4
2 User	5
2.1 Request a user certificate (CSR).....	5
2.2 Request a service/server certificate (CSR).....	9
2.3 Get the signed certificate.....	13
2.4 Revoke Certificate.....	17
2.5 Export/Backup certificates.....	21
3 CA	24
3.1 Get CA certificate.....	24
3.2 Certification Revocation Lists (CRLs).....	26
4 pkIRISGrid Policy.....	26

History

Date	Version	Changes	Owner
21/06/2008	1.5	New version of template document	Juan Carlos Sánchez Del Barrio
10/12/2010	1.6	Modify URIs	Juan Carlos Sánchez Del Barrio

1 Introduction

This document describes the use of the web interface to *pkIRISGrid*. *pkIRISGrid* (<http://pki.irisgrid.es/>) emits person, host and server PKI certificates for the members of the RedIRIS community. Through the web interface, users can issue certificates requests (CSR), revoke their own certificates, and download CA and revocation certificates.

Barcelona Supercomputing Center – Centro Nacional de Supercomputación (BSC-CNS) acts as Registration Authority (RA) of the *pkIRISGrid*. The web interface to BSC-CNS RA can be accessed at the following url: <https://pki.irisgrid.es/rat4/>

The *pkIRISGrid Policy* is available at the same url: <https://pki.irisgrid.es/rat4/>.

1.1 BSC-CNS RA Policy Restrictions

See document <https://pki.irisgrid.es/rat4/policy/>.

2 User

This section allows the user to manage their certificates. It allows certificate request, retrieval and revocation.

2.1 Request a user certificate (CSR)

Go to *pkIRISGrid Public Interface* (<https://pki.irisgrid.es/rat4/>) using Mozilla Web Browser (or Firefox). You can access *Public Interface* as an anonymous user.

1. Click on the “*CSR de Usuario: con Mozilla*” and prepare a person certificate request.



- Fill in the form and submit the data (click on the “Continuar” button). The data submitted will be used to create a certificate signing request (CSR) which will be sent to the Certificate Authority (CA) to be signed and returned as a certificate.

RedIRIS - Solicitud de certificado para IRISGrid - para Mozilla y compatibles (SPKAC) - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

https://rat4.irisgrid.es/csr_spkac.phtml?eet=usr

NOVELL: Support Entertainment News Internet Search Reference Maps and Directions Shopping People and Compani...

IRISGrid < pkIRISGrid

Solicitud de certificado para IRISGrid para Mozilla y compatibles (SPKAC)

Autoridad de Registro: BSC-CNS

Identificador IRISGrid: jcarlos.sanchez @ bsc.es

Nombre: Juan Carlos

Apellidos: Sanchez Del Barrio

Clave de Usuario: *****

Teléfono: +34 XXX XX XX

email: xxx@bsc.es

PIN para certificado: *****

Repite PIN: *****

Continuar

Actualizado el 05/12/2005 RedIRIS © 1994-2005

The form data has the following fields:

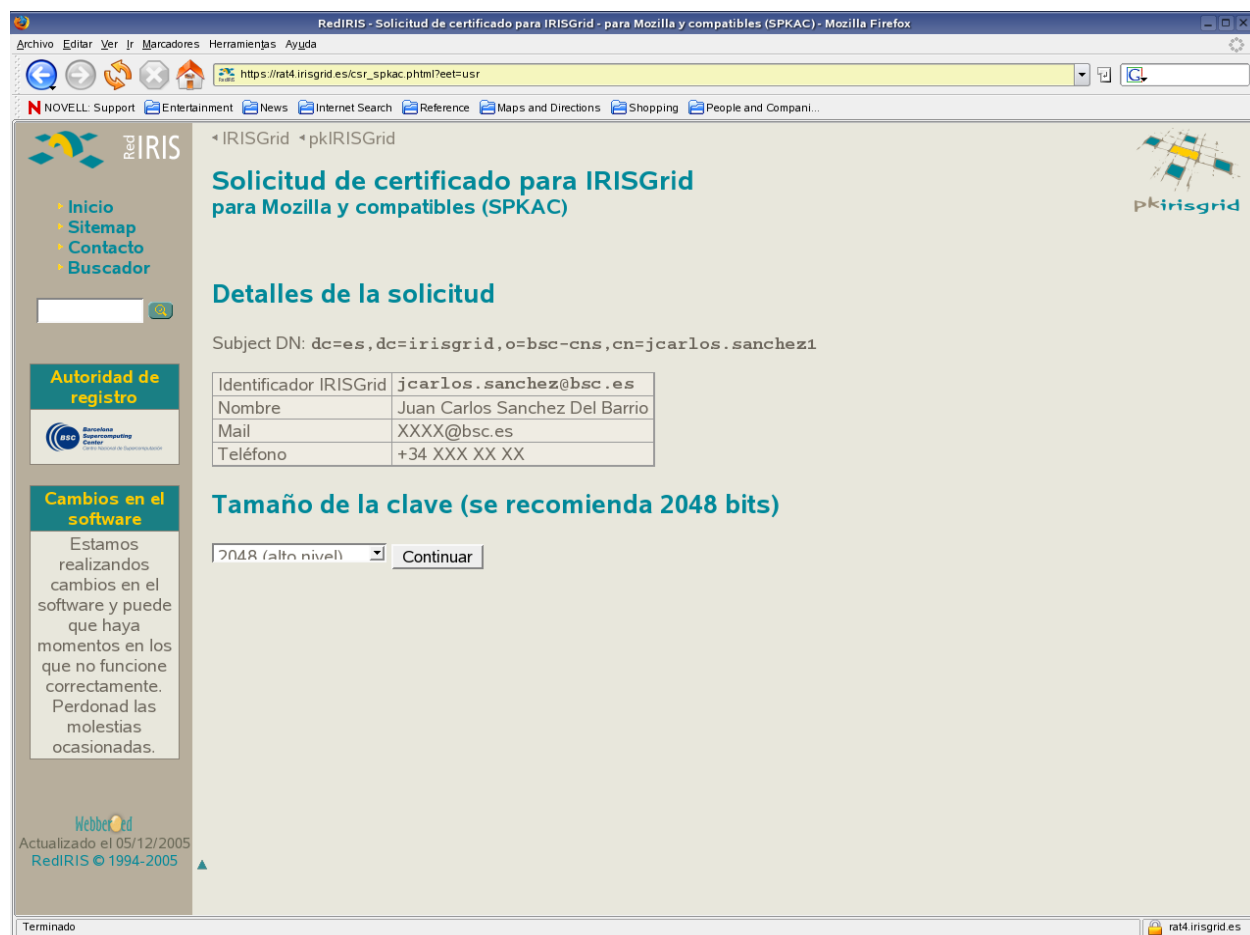
- Identificador IRISGrid*: The internal identification associated with the certificate¹.
- Nombre*: The name of the user².
- Apellidos*: The surname of the user².
- Clave de Usuario*: A password used to manage the certificate (e.g.: renew the certificate).
- Teléfono*: A telephone number of the user².
- Email*: The email address associated with the user².

¹ Must have the format: name.first_surname[.second_surname] (the domain will always be bsc.es).

² These fields must have TRUE values, and they will be verified by BSC-CNS RA agent. Note that this information will not appear in the certificate, it will be used for CA/RA management purposes only and will not be used or communicated outside this context.

- *PIN*: A password used to verify the CSR, or revoke the signed certificate.

3. Verify the request details and Click on the “Continuar” button.



4. The request certificate has been generated by SPKAC system from Mozilla. Save your “Código de solicitud”. This code is the ticket of the certificate in the *pkIRISGrid* system.



The screenshot shows a Mozilla Firefox browser window with the URL `https://rat4.irisgrid.es/csr_add.phtml`. The page title is "Solicitud de Certificado para IRISGrid". The main content area displays "Solicitud aceptada" and "Su solicitud:" followed by a table:

DN	dc=es,dc=irisgrid,o=bsc-cns,cn=jcarlos.sanchez
Identificador IRISGrid	jcarlos.sanchez@bsc.es
Código solicitud	a4b15c1

Below the table, it states "ha sido aceptada." and "Por favor, es muy importante que anote los valores anteriores ya que le serán de utilidad a la hora de las siguientes operaciones:" followed by a list of actions:

- Autenticación frente a la autoridad de registro
- Descarga de su certificado
- Revocación de su certificado

The left sidebar contains navigation links: Inicio, Sitemap, Contacto, and Buscador. There is also a search box and a section titled "Cambios en el software" with a message about software updates. The footer includes "Webberd Actualizado el 05/12/2005 RedIRIS © 1994-2005".

5. Contact with an RA agent to validate your certificate request. You will have 9 days to identify yourself for this certificate request to be approved. (See BSC-CNS RA Policy on section 1).

2.2 Request a service/server certificate (CSR)

Go to *pkIRISGrid Public Interface* (<https://pki.irisgrid.es/rat4/>) using Mozilla Web Browser (or Firefox). You can access *Public Interface* as anonymous user.

1. Click on the “*CSR de Servidor/Servicio: con Mozilla*” and prepare a service/server certificate request.

The screenshot shows a Mozilla Firefox browser window displaying the website <https://rat4.irisgrid.es/>. The page title is "RedIRIS - pkIRISGrid - PKI para IRISGrid - V0.2 beta - Mozilla Firefox". The browser's address bar shows the URL. The website content includes a navigation menu on the left with links for "Inicio", "Sitemap", "Contacto", and "Buscador". Below the navigation menu, there are sections for "Autoridad de registro" and "Cambios en el software". The main content area features a breadcrumb trail "IRISGrid > pkIRISGrid" and a heading "pkIRISGrid - PKI para IRISGrid V0.2 beta". Underneath, it says "Usuario · RA · CA". The "Usuario" section contains a list of links: "Elección de la autoridad de registro más cercana", "Solicitud de certificado (CSR):" (with sub-links for "CSR de Usuario: con Mozilla - con IE" and "CSR de Servidor/Servicio: con Mozilla - con IE"), "Descarga del certificado solicitado (una vez firmado por la CA)", "¿Cómo usar el certificado con Globus?", "Revocar certificado", and "Ayuda". The "Autoridad de Certificación IRISGrid" section includes links for "Política", "Obtención del Certificado de la CA", and "Listas de Revocación de Certificados" (with sub-links for "pkIRISGrid CRL - formato PEM" and "pkIRISGrid CRL - formato texto (puede ser muy grande)"). The footer of the page mentions "Webbexid", "Actualizado el 29/11/2005", and "RedIRIS © 1994-2005". The browser's status bar at the bottom shows "Parado" and the address "rat4.irisgrid.es".

2. Fill in the form and submit the data (click on the “Continuar” button). The data submitted will be used to create a certificate signing request (CSR) which will be sent to the Certificate Authority (CA) to be signed and returned as a certificate.

RedIRIS - Solicitud de certificado para IRISGrid - para Mozilla y compatibles (SPKAC) - Mozilla Firefox

Inicio
Sitemap
Contacto
Buscador

Autoridad de registro

Cambios en el software

Estamos realizando cambios en el software y puede que haya momentos en los que no funcione correctamente. Perdonad las molestias ocasionadas.

Webbated
Actualizado el 05/12/2005
RedIRIS © 1994-2005

pkirisgrid

Solicitud de certificado para IRISGrid para Mozilla y compatibles (SPKAC)

Autoridad de Registro: BSC-CNS

Identificador IRISGrid: / .

Datos del Responsable

Nombre:

Apellidos:

Clave de Usuario:

Teléfono:

email:

PIN para certificado:

Repite PIN:

https://rat4.irisgrid.es/help.phtml#clave_usuario

The form data has the following fields:

- *Identificador IRISGrid*: The internal identification associated with the certificate³.
- *Nombre*: The name of the applicant (system responsible)⁴.
- *Apellidos*: The surname of the applicant (system responsible)⁴.
- *Clave de Usuario*: A password used to manage the certificate (e.g.: renew the certificate)⁵.
- *Teléfono*: the phone number of the applicant⁴.
- *Email*: The email address of the applicant⁴.
- *PIN*: A password used to verify the CSR or revoke the signed certificate⁵.

3. Verify the request details and Click on the “Continuar” button.

The screenshot shows a web browser window with the URL https://rat4.irisgrid.es/csr_spkac.phtml?eet=svr. The page title is "Solicitud de certificado para IRISGrid para Mozilla y compatibles (SPKAC)". The main content area is titled "Detalles de la solicitud" and displays the following information:

Subject DN: dc=es,dc=irisgrid,o=bsc-cns,cn=ldap/BSCSI10.bsc.es

Identificador IRISGrid	ldap/BSCSI10.bsc.es
------------------------	---------------------

Datos del Responsable

Nombre	Juan Carlos Sanchez Del Barrio
Mail	*****@bsc.es
Teléfono	+34 *****

Tamaño de la clave (se recomienda 2048 bits)

2048 (alto nivel)

On the left side of the page, there is a sidebar with navigation links: Inicio, Sitemap, Contacto, and Buscador. Below these are sections for "Autoridad de registro" (BSC-CNS) and "Cambios en el software" (software updates). The footer includes the WebberCid logo and the text "Actualizado el 05/12/2005 RedIRIS © 1994-2005".

3 Must have the format: service/server name or server name; the domain must be chosen from the given list. The resulting host name must be a fully qualified domain name (FQDN); alias are not accepted.

4 These fields must have TRUE values, as will be verified by a BSC-CNS RA agent.

5 Note that this password is associated to the *IRISGrid* identifier, not to the applicant. Therefore, BSC-CNS RA encourages administration teams to have a clear policy on saving these passwords and the procedure to follow when the system responsible changes.

4. The request certificate has been generated by SPKAC system from Mozilla. Save your “Código de solicitud”. This code is the ticket of the certificate in the *pkIRISGrid* system.



5. Validate your request certificate (see BSC-CNS RA Policy in section 1 of this document).

2.3 Get the signed certificate

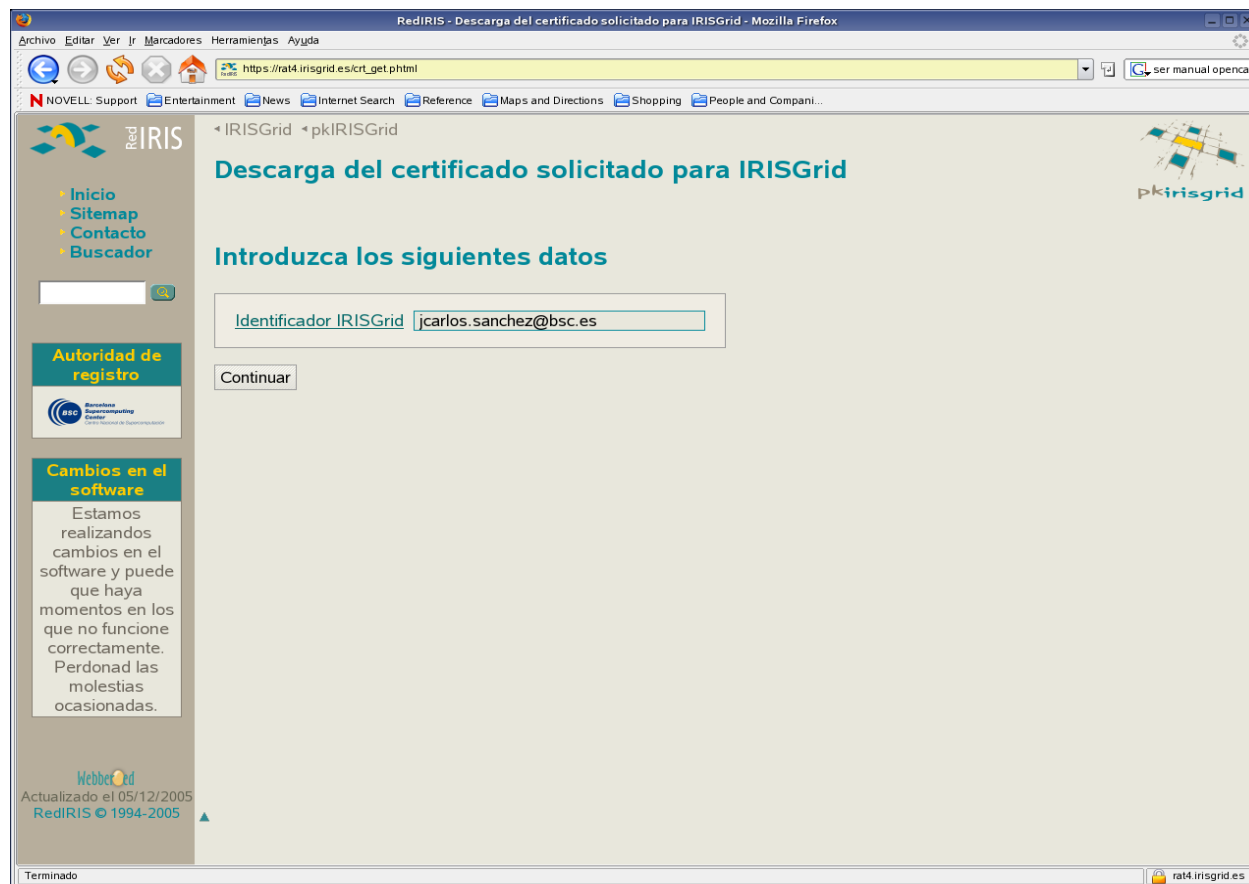
The signed certificate must be retrieved from the same web browser (in the same computer) used to issue the certificate request (CSR). This is important because the web browser needs to link the certificate back to the CSR and private keys, and this can be done in the browser where the CSR was generated only.

1. Click on the “*Descarga*” link when you receive email response from *pkIRISGrid CA* validating requested certificate.



The screenshot shows a Mozilla Firefox browser window displaying the website <https://rat4.irisgrid.es/>. The page title is "pkIRISGrid - PKI para IRISGrid V0.2 beta". The navigation menu includes "Inicio", "Sitemap", "Contacto", and "Buscador". The main content area is titled "Usuario" and lists several links: "Elección de la autoridad de registro más cercana", "Solicitud de certificado (CSR):" (with sub-links for "con Mozilla - con IE" and "con Mozilla - con IE"), "Descarga del certificado solicitado (una vez firmado por la CA)", "¿Cómo usar el certificado con Globus?", "Revocar certificado", and "Ayuda". Below this is the "Autoridad de Certificación IRISGrid" section with links for "Política", "Obtención del Certificado de la CA", and "Listas de Revocación de Certificados" (with sub-links for "pkIRISGrid CRL - formato PEM" and "pkIRISGrid CRL - formato texto (puede ser muy grande)"). A sidebar on the left contains "Autoridad de registro" and "Cambios en el software" (with a notice about software updates). The footer includes "Webbated" and "Actualizado el 29/11/2005 RedIRIS © 1994-2005".

2. Introduce the corresponding “*Identificador IRISGrid*” and Click the “*Continuar*” button.



- Click on the "Instalar su certificado en el navegador" button to install the certificate in the navigator. Upon pressing the "Instalar su certificado en el navegador" button, the *pkIRISGrid* system attempts to install the certificate into the user's browser.

Red IRIS

- Inicio
- Sitemap
- Contacto
- Buscador

Autoridad de registro

Cambios en el software

Estamos realizando cambios en el software y puede que haya momentos en los que no funcione correctamente. Perdonad las molestias ocasionadas.

Descarga del certificado solicitado para IRISGrid

Datos sobre la solicitud del certificado (CSR)

DN	dc=es,dc=irisgrid,o=bsc-cns,cn=jcarlos.sanchez
Identificador IRISGrid	jcarlos.sanchez@bsc.es
Nombre	Juan Carlos Sanchez Del Barrio
Número de serie de la CSR	a4b14c1
Tipo	Certificado de usuario

Para instalar el certificado en su navegador es necesario que utilice el mismo navegador desde el que realizó la petición del certificado. En caso contrario no podrá instalarlo

[Instalar su certificado en el navegador](#)

Datos sobre el certificado que va a descargar

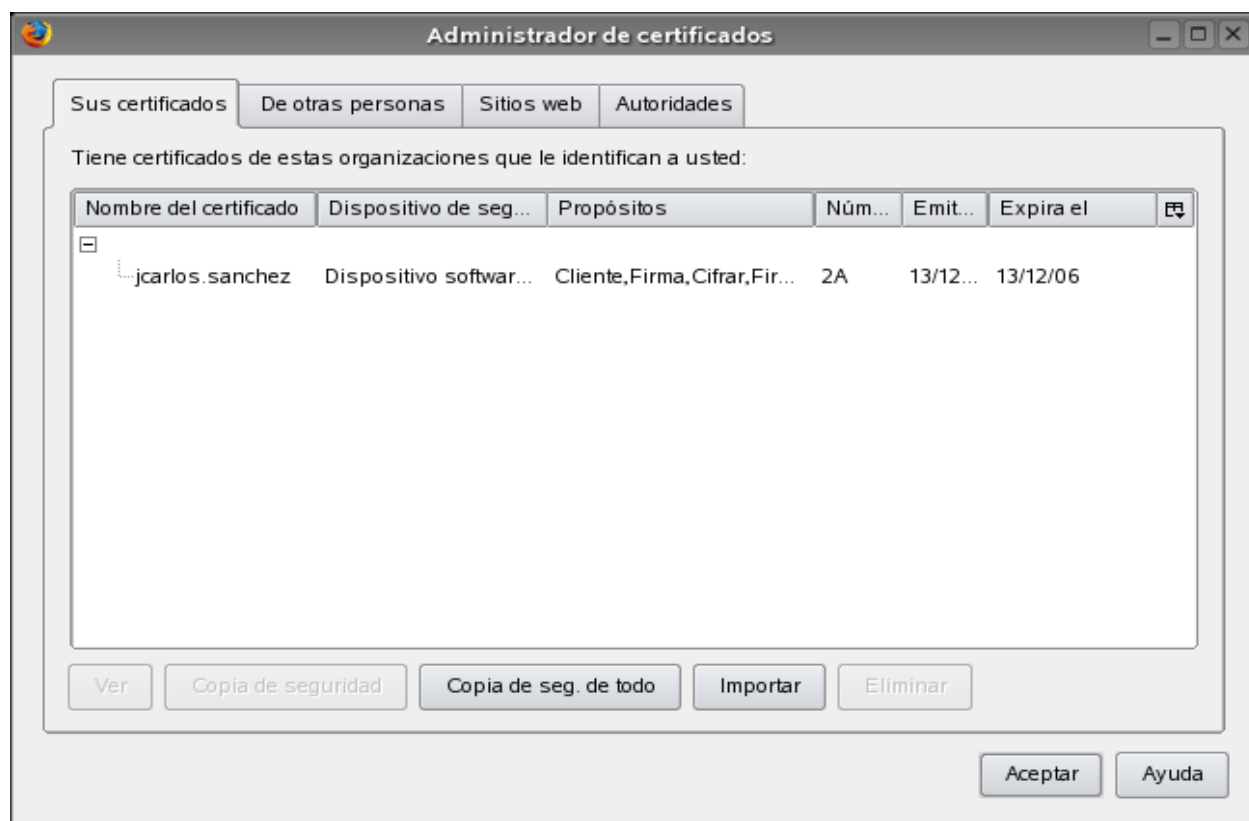
Certificate:

```

Data:
  Version: 3 (0x2)
  Serial Number: 42 (0x2a)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: DC=es, DC=irisgrid, CN=IRISGridCA
  Validity
    Not Before: Dec 13 10:36:37 2005 GMT
    Not After : Dec 13 10:36:37 2006 GMT
  Subject: DC=es, DC=irisgrid, O=bsc-cns, CN=jcarlos.sanchez
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
    Modulus (2048 bit):
      00:d0:49:d5:f8:17:81:a0:d5:bd:08:df:ce:b7:91:
      67:0a:31:bd:0b:c9:bb:b3:ac:3d:22:df:3a:48:10:
      a2:6d:5c:97:58:8d:90:7d:c6:c3:e6:5f:38:16:0b:
      a8:5f:a9:c8:f7:82:6a:3d:4e:2a:03:9e:9a:e2:86:
      a4:e9:0c:d7:f9:41:38:b6:13:45:33:b6:c3:f1:a8:
      ed:11:c6:7d:c4:9f:18:e2:97:19:87:fe:cd:20:5b:
      94:d0:9d:9d:f7:e5:9d:a2:4f:fe:39:11:fb:ab:cl:
      05:a2:c2:84:84:c8:fd:94:ac:46:2a:89:e5:d5:18:
      2d:18:18:2c:4c:3a:4b:89:08:18:ab:66:ea:6a:b0:
      0d:b6:97:10:68:85:30:8b:32:d8:7c:a1:bb:3a:ad:
      91:67:59:a1:57:4e:12:6a:2d:c5:90:ef:70:e8:b1:
      24:4a:a1:a3:76:72:d6:af:f8:6f:0e:0f:54:a6:28:
      54:e0:31:79:ad:ed:18:90:bb:3a:1e:4a:88:5c:70:
      e1:83:3c:17:5a:82:82:ef:7d:ba:77:f9:ac:bd:39:
  
```

Terminado

4. To verify that the certificate is installed correctly, Go to “*Editar-->Preferencias--> Avanzadas--> Certificados-->Administrador de Certificados-->Sus Certificados*” on the Mozilla Web Browser.



2.4 Revoke Certificate

1. Click on the “*Revocar Certificado*” link.



The screenshot shows a web browser window displaying the RedIRIS website. The page title is "pkIRISGrid - PKI para IRISGrid V0.2 beta". The main content area is titled "Usuario" and contains a list of links for users, including "Elección de la autoridad de registro más cercana", "Solicitud de certificado (CSR)", "Descarga del certificado solicitado", "¿Cómo usar el certificado con Globus?", "Revocar certificado", and "Ayuda". The "Revocar certificado" link is highlighted in blue. The page also features a sidebar with navigation links like "Inicio", "Sitemap", "Contacto", and "Buscador", and a section titled "Cambios en el software" with a notice about software updates. The footer includes the RedIRIS logo and the text "Actualizado el 29/11/2005 RedIRIS © 1994-2005".

2. Users have the opportunity to revoke their own certificates. To do this they need to fill in the form and click on the "Continuar" button.



3. Click on the “Solicitar la revocación” button.

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

https://rat4.irisgrid.es/crr.phtml

NOVELL: Support Entertainment News Internet Search Reference Maps and Directions Shopping People and Compani...

Red IRIS

- Inicio
- Sitemap
- Contacto
- Buscador

Autoridad de registro

Cambios en el software

Estamos realizando cambios en el software y puede que haya momentos en los que no funcione correctamente. Perdonad las molestias ocasionadas.

pkirisgrid

Solicitud de revocación de certificado para IRISGrid

Detalles de la solicitud de revocación del certificado

Identificador IRISGrid	jcarlos.sanchez@bsc.es
Identificador del certificado	a4b15c1

Detalles del certificado a revocar

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number: 45 (0x2d)
Signature Algorithm: sha1WithRSAEncryption
Issuer: DC=es, DC=irisgrid, CN=IRISGridCA
Validity
  Not Before: Dec 14 08:09:24 2005 GMT
  Not After : Dec 14 08:09:24 2006 GMT
Subject: DC=es, DC=irisgrid, O=bsc-cns, CN=jcarlos.sanchez
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
  Modulus (2048 bit):
    00:be:b3:fc:e5:8f:27:27:3f:f0:66:7f:1b:18:ab:
    9f:f0:77:34:96:64:79:5c:12:df:51:f9:7e:97:0e:
    a2:ff:ff:c9:f4:cb:ee:49:54:1d:28:87:ff:97:a1:
    49:f4:f9:ef:7f:5f:37:bb:4b:b7:77:e7:ca:bf:55:
    63:cc:2e:35:e6:d9:32:92:d3:ed:2e:de:5a:08:77:
    76:c0:78:40:aa:18:a7:d6:34:d7:b8:32:f2:e6:66:
    7a:d4:ee:75:62:e5:c6:7e:a5:cd:5c:cb:57:5b:4d:
    5c:0e:ad:c6:05:82:a5:cc:fe:86:bc:af:b6:9b:bc:
    a7:5d:ed:54:f8:e3:e0:4c:14:05:68:88:f2:6b:1b:
    1a:fa:89:09:50:8e:94:09:17:1e:ec:2b:38:bb:80:
    de:84:31:ee:b9:4e:28:12:2e:49:eb:2b:1f:d2:fb:
    46:bf:8c:58:58:fe:dd:e7:19:e7:4e:fb:b5:39:13:
    26:0f:32:6d:b2:79:62:bb:31:de:97:a3:25:28:33:
    90:57:c2:76:66:dc:52:c6:26:3e:6a:fa:3e:c9:9b:
```

Terminado

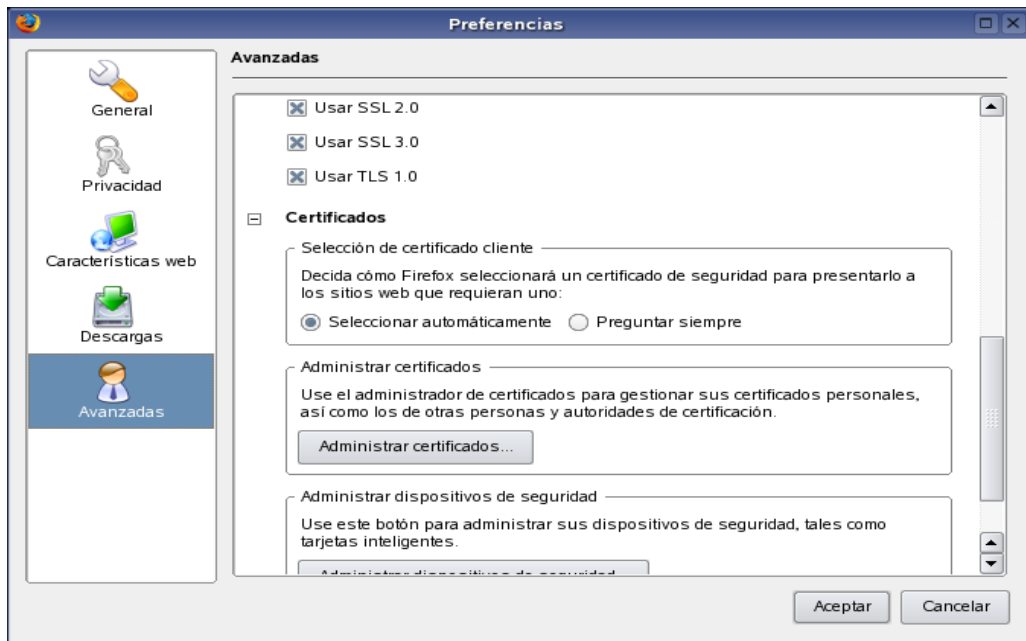
rat4 irisgrid es

4. *pkIRISGrid* sends your revocation request to certificate revocation requests list (CRRL).

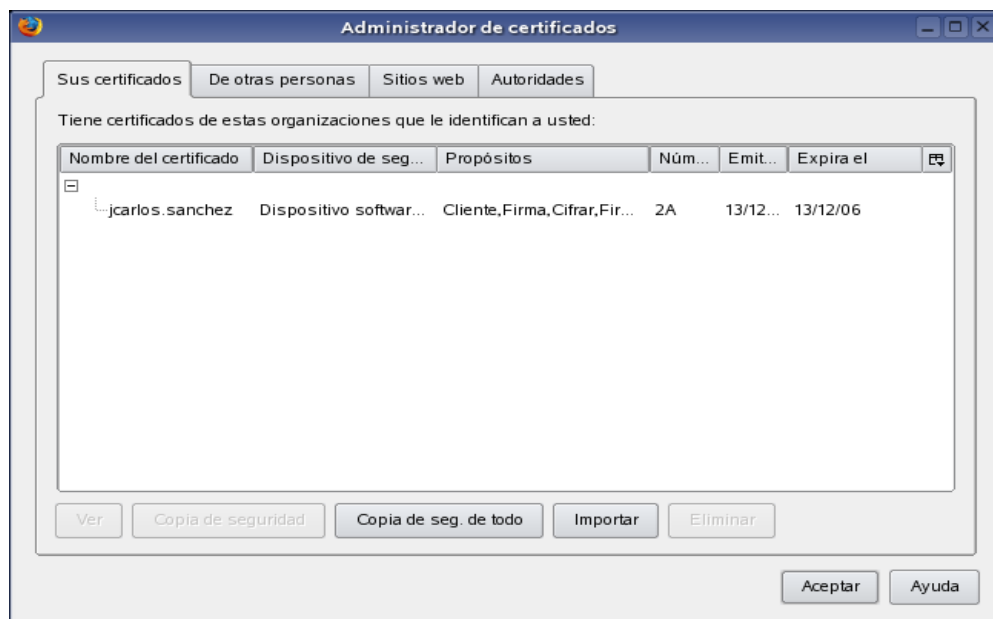


2.5 Export/Backup certificates

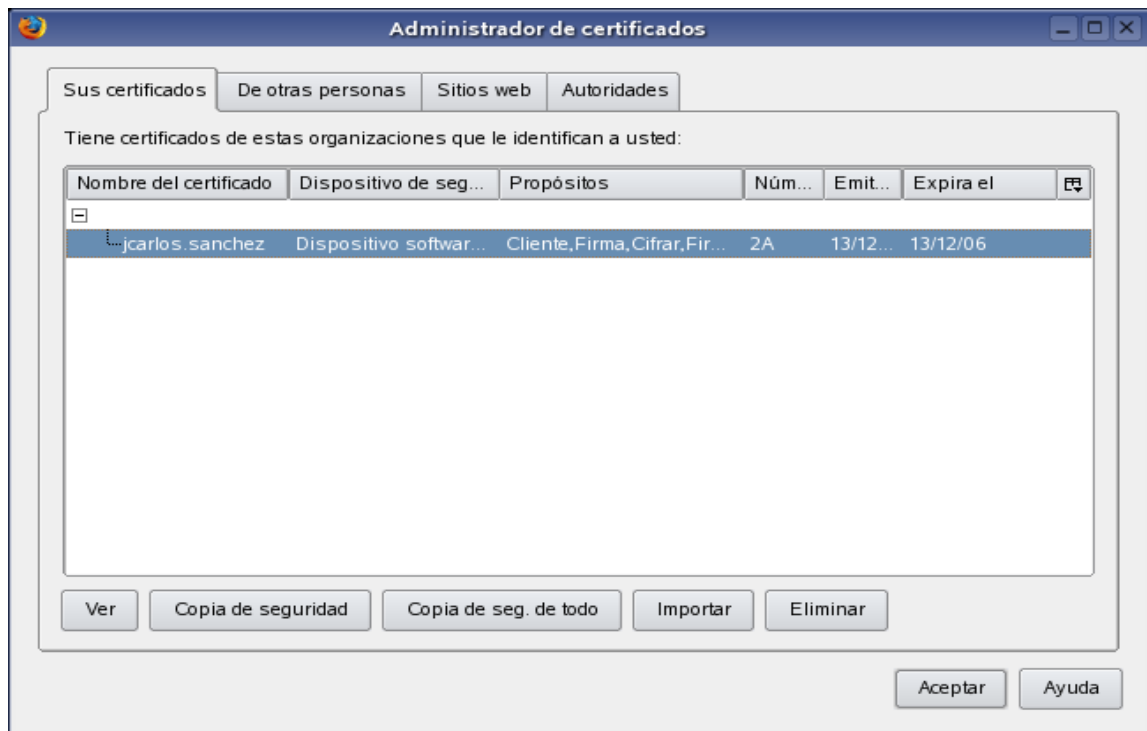
1. From the “*Editar*” menu select “*Preferencias*” and open the “*Avanzadas*” category and click on the “*Certificados*” item.



2. In the “*Administrador certificados*” section, click on the “*Administrar certificados...*” button. In the “*Administrador certificados*” window the “*Sus certificados*” tab should automatically open (if not, select it).



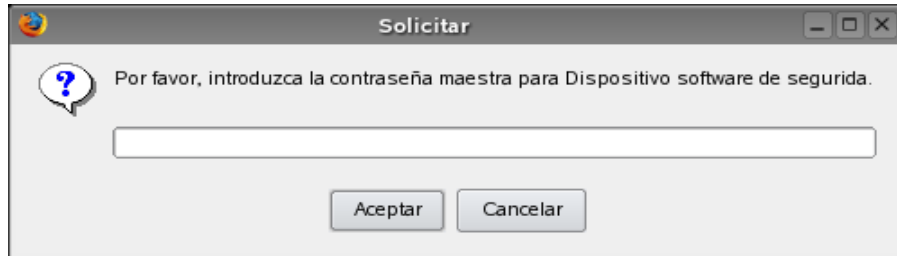
- To export your personal certificate, click on it to select it, and click the “Copia de seguridad” button at the bottom of the window.



- You'll be prompted to specify a filename and location for the *PKCS#12-format certificate file* (file extension will be **.p12** in UNIX/Linux, **.pfx** in Windows). Provide them and click “Guardar”.



5. A dialog box requesting the “*contraseña maestra*” may appear (the password and certificate database). If you have set a “*contraseña maestra*”, provide it. If not, you can make one up and provide it (optional). Remember this password!



6. You'll be prompted to make up and (twice) enter a second password. This one is for restoring this particular backup of this certificate. Remember this password!



7. Once the system says it's successfully backed up your certificate and private key, click “*Aceptar*”.



3 CA

This section describes the CA related utilities a user can access.

3.1 Get CA certificate

In order for the user/server to "trust" certificates generated through *pkIRISGrid* they must have the Certificate Authority (CA) root certificate installed.

1. Click on the "Obtención del Certificado de la CA" link.



The screenshot shows a Mozilla Firefox browser window displaying the website <https://rat4.irisgrid.es/>. The page title is "pkIRISGrid - PKI para IRISGrid V0.2 beta". The browser's address bar shows the URL, and the status bar at the bottom indicates "Parado" and "rat4.irisgrid.es".

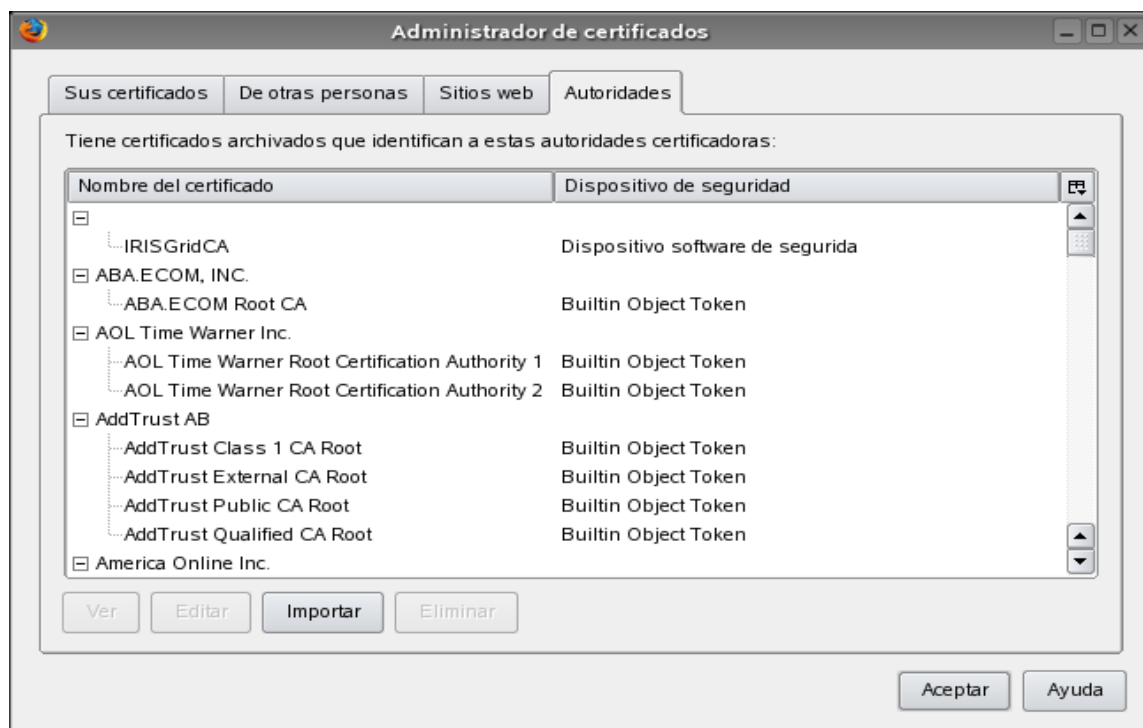
The website content includes:

- Navigation:** Inicio, Sitemap, Contacto, Buscador.
- Autoridad de registro:** Logo of the Spanish Data Protection Agency (Agencia Española de Protección de Datos).
- Cambios en el software:** A notice stating: "Estamos realizando cambios en el software y puede que haya momentos en los que no funcione correctamente. Perdonad las molestias ocasionadas." It is dated "Actualizado el 29/11/2005" and "RedIRIS © 1994-2005".
- Usuario:** A section for user actions, including:
 - Elección de la [autoridad de registro](#) más cercana
 - Solicitud de certificado (CSR):
 - CSR de Usuario: [con Mozilla](#) - con IE
 - CSR de Servidor/Servicio: [con Mozilla](#) - con IE
 - [Descarga](#) del certificado solicitado (una vez firmado por la CA)
 - [¿Cómo usar el certificado con Globus?](#)
 - [Revocar](#) certificado
 - [Ayuda](#)
- Autoridad de Certificación IRISGrid:** A section for CA-related information, including:
 - [Política](#)
 - Obtención del [Certificado de la CA](#)
 - Listas de Revocación de Certificados:
 - [pkIRISGrid CRL](#) - formato PEM
 - [pkIRISGrid CRL](#) - formato texto (puede ser muy grande)

2. Check all boxes and Click on the “Aceptar” button.



3. To check if the CA certificate is installed correctly, Go to “*Editar-->Preferencias-->Avanzadas-->Certificados-->Administrador de Certificados-->Autoridades*” on the Mozilla Web Browser.



3.2 Certification Revocation Lists (CRLs)

Many certificate aware clients (like Microsoft Outlook, Netscape Navigator and Mozilla Web Browser) make use of certificate revocation lists to ensure that certificates are still valid and have not been revoked.

1. Save link “*pkIRISGrid CRL – formato PEM*” as PEM file.



4 pkIRISGrid Policy

<http://pki.irisgrid.es/ca/policy/>