Barcelona Supercomputing Center
Centro Nacional de Supercomputación

BSC-CNS pkIRISGrid User Manual

Version: 1.6

Barcelona, 10. Dec. 2010

Table of Contents

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*. P*kIRISGrid* (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/.

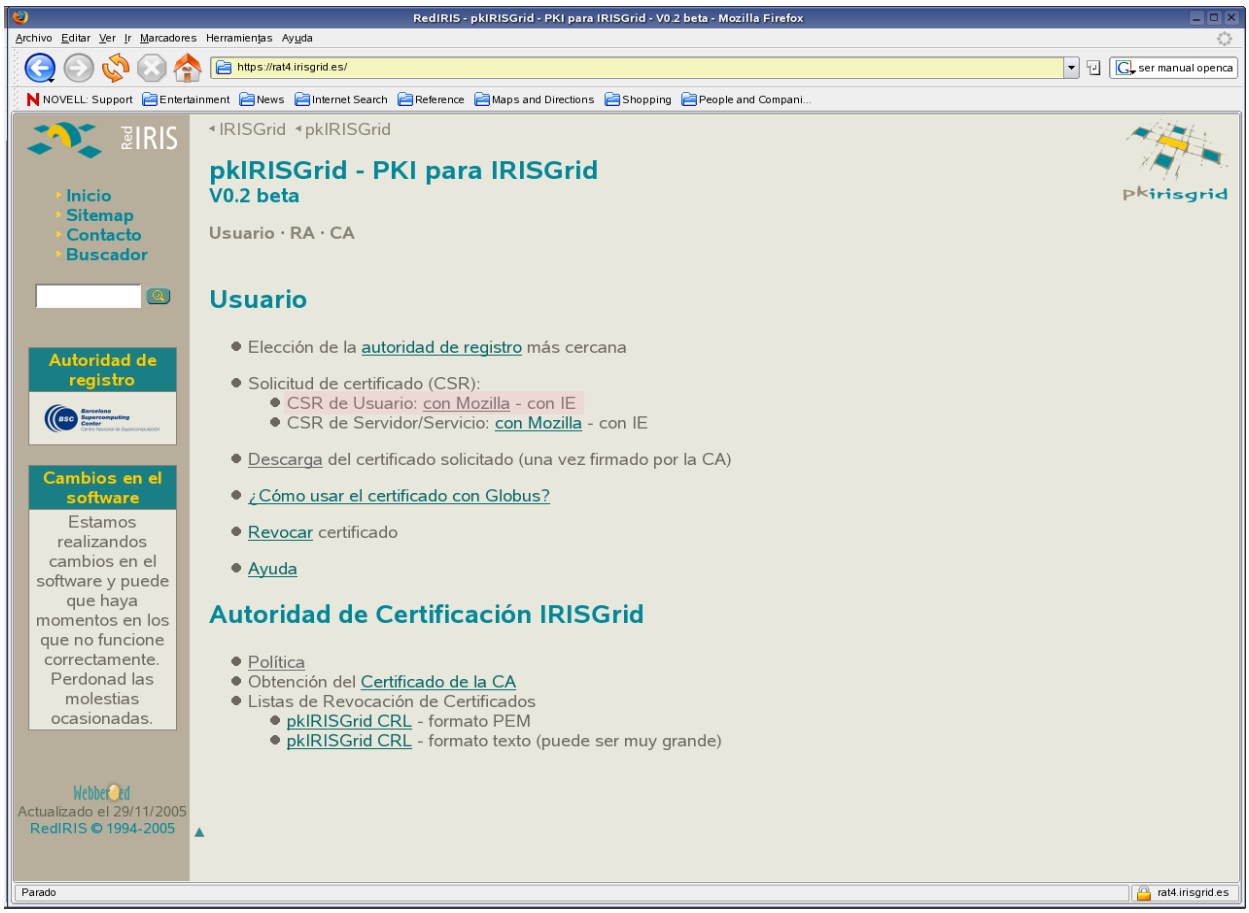
2 User

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

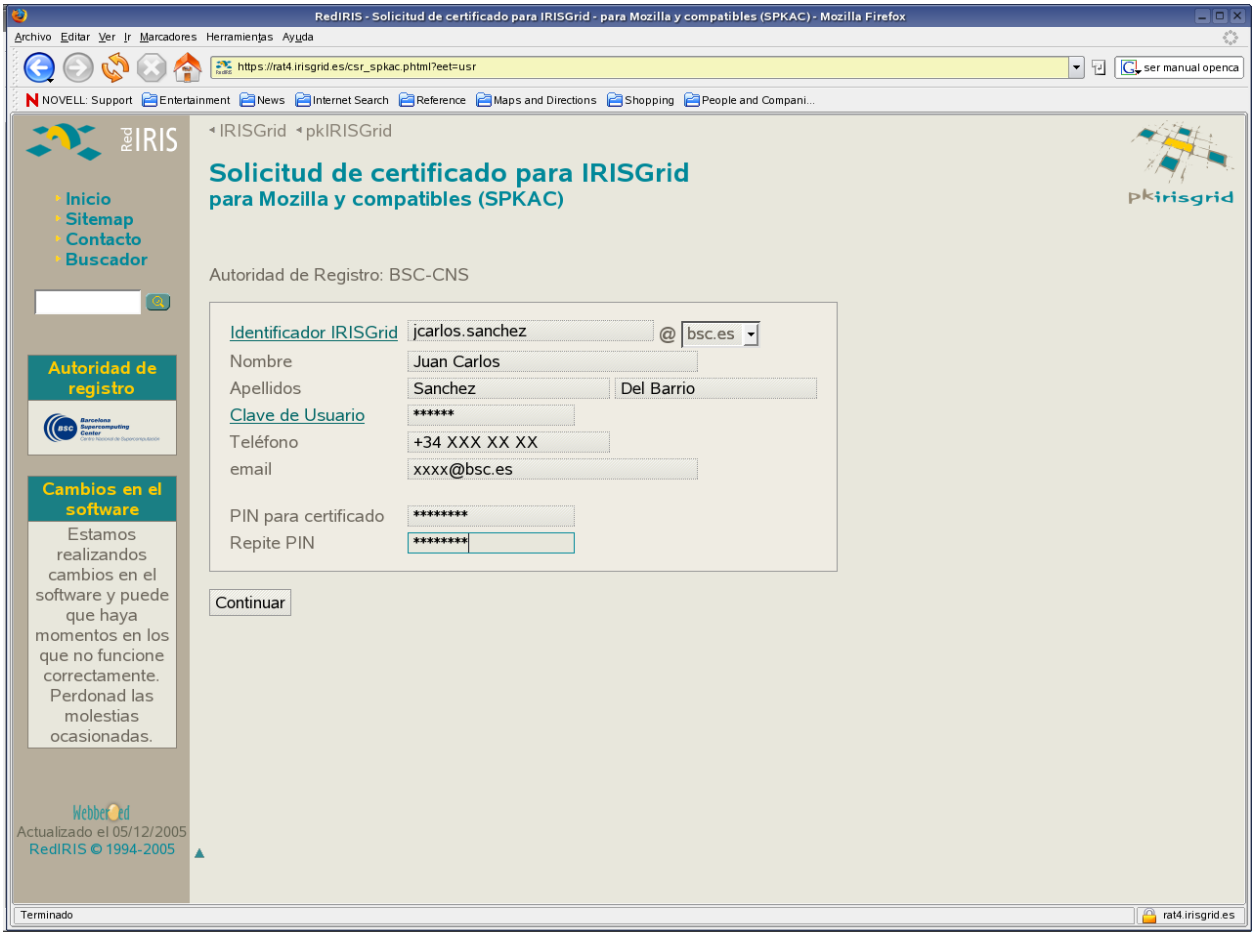
2.1 Request a user certificate (CSR)

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.



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 signed and returned as a certificate.



The form data has the following fields:

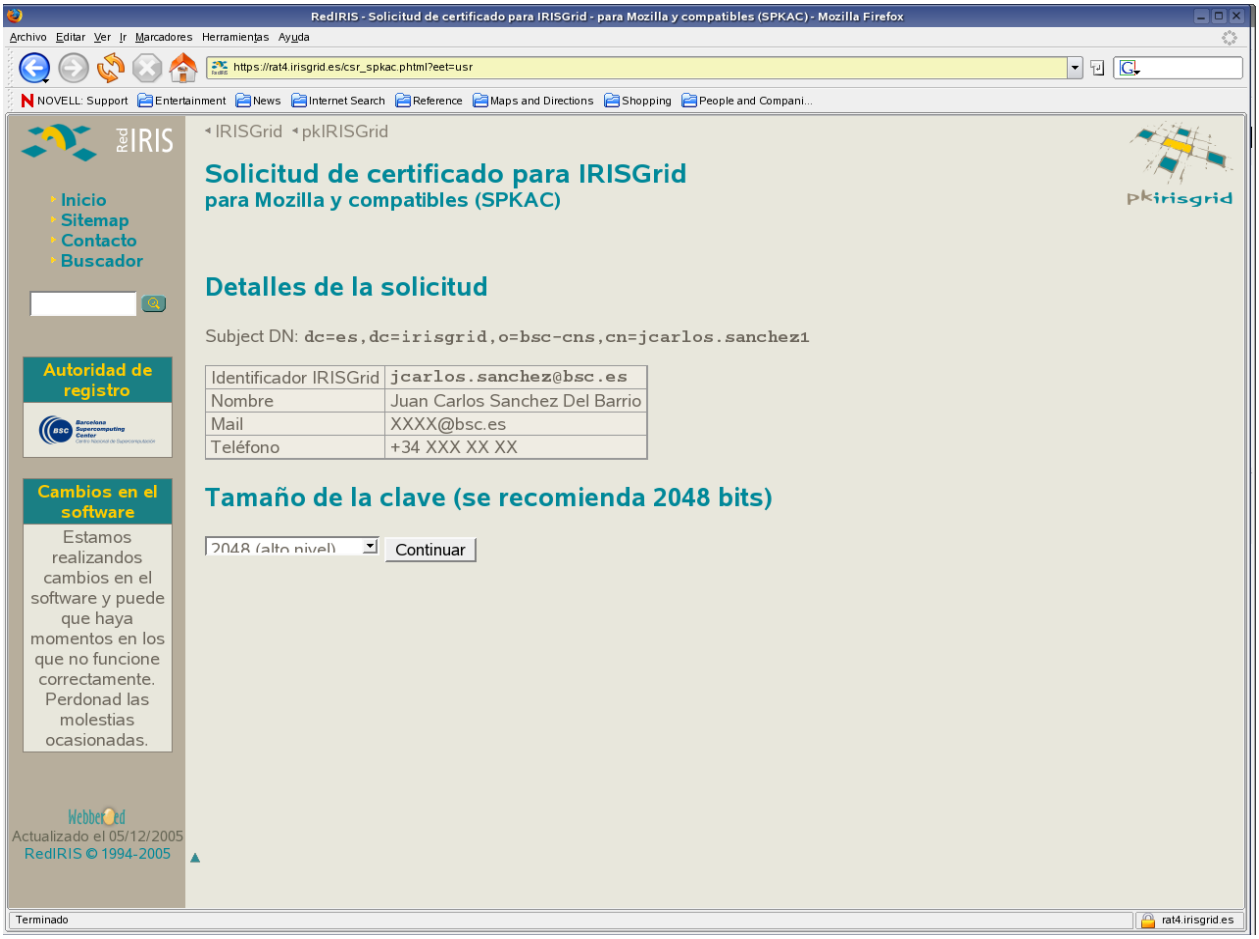
- *Identificador IRISGrid*: The internal identification associated with the certificate[1].
- *Nombre*: The name of the user[2].
- *Apellidos*: The surname of the user[2].
- *Clave de Usuario*: A password used to manage the certificate (e.g.: renew the certificate).
- *Teléfono*: A telephone number of the user[2].
- *Email*: The email address associated with the user[2] .

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*.

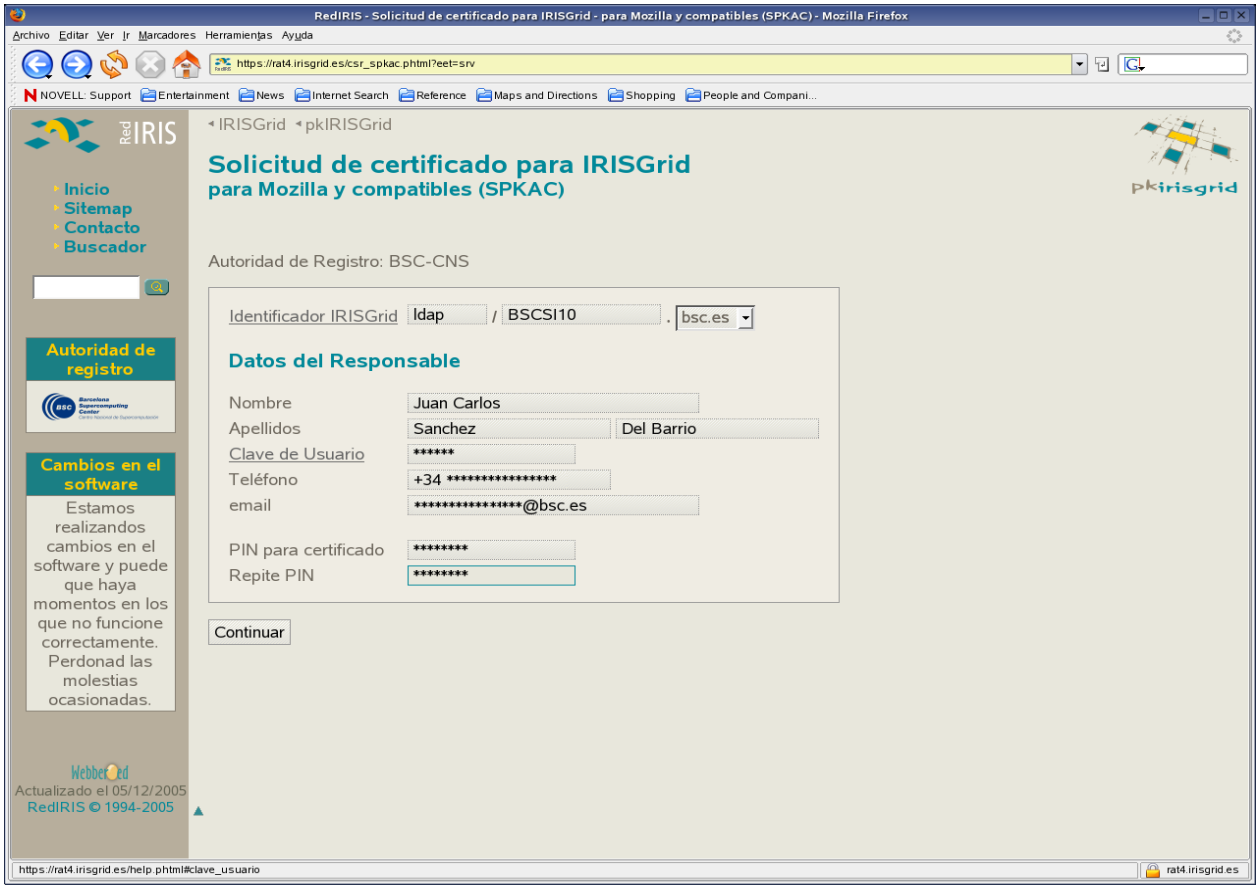
5. Contact with an RA agent to validate your certificate request. You will have 9 days to identify yourself for this certificate request to be approved. (See BSC-CNS RA Policy on section 1).

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.

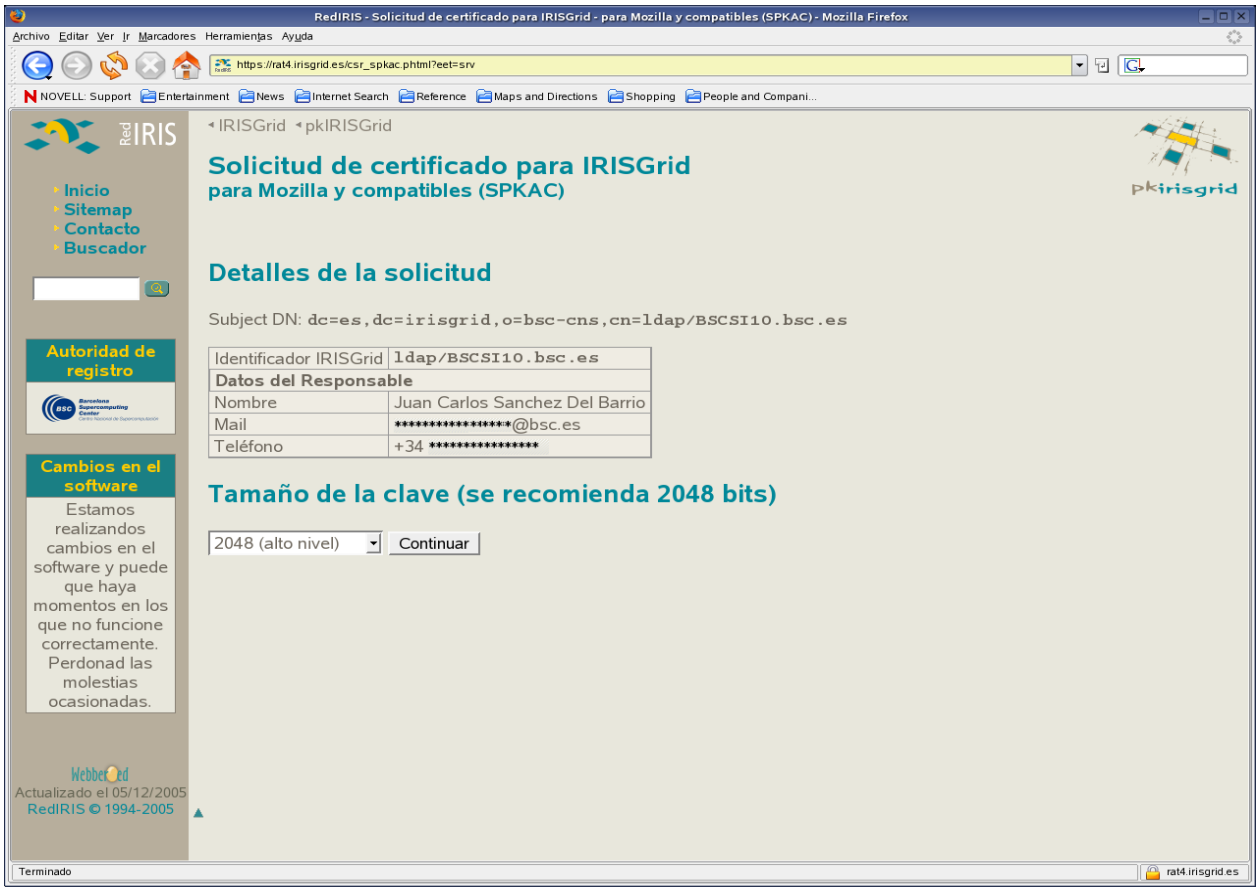
2. Fill in the form and submit the data (click on the "*Continuar*" button). The data submitted will be used to create a certificate signing request (CSR) which will be sent to the Certificate Authority (CA) to be signed and returned as a certificate.



The form data has the following fields:

- *Identificador IRISGrid*: The internal identification associated with the certificate[3].
- *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 applicant[4].
- *Email*: The email address of the applicant[4].
- *PIN*: A password used to verify the CSR or revoke the signed certificate[5].

3. Verify the request details and Click on the "*Continuar*" button.

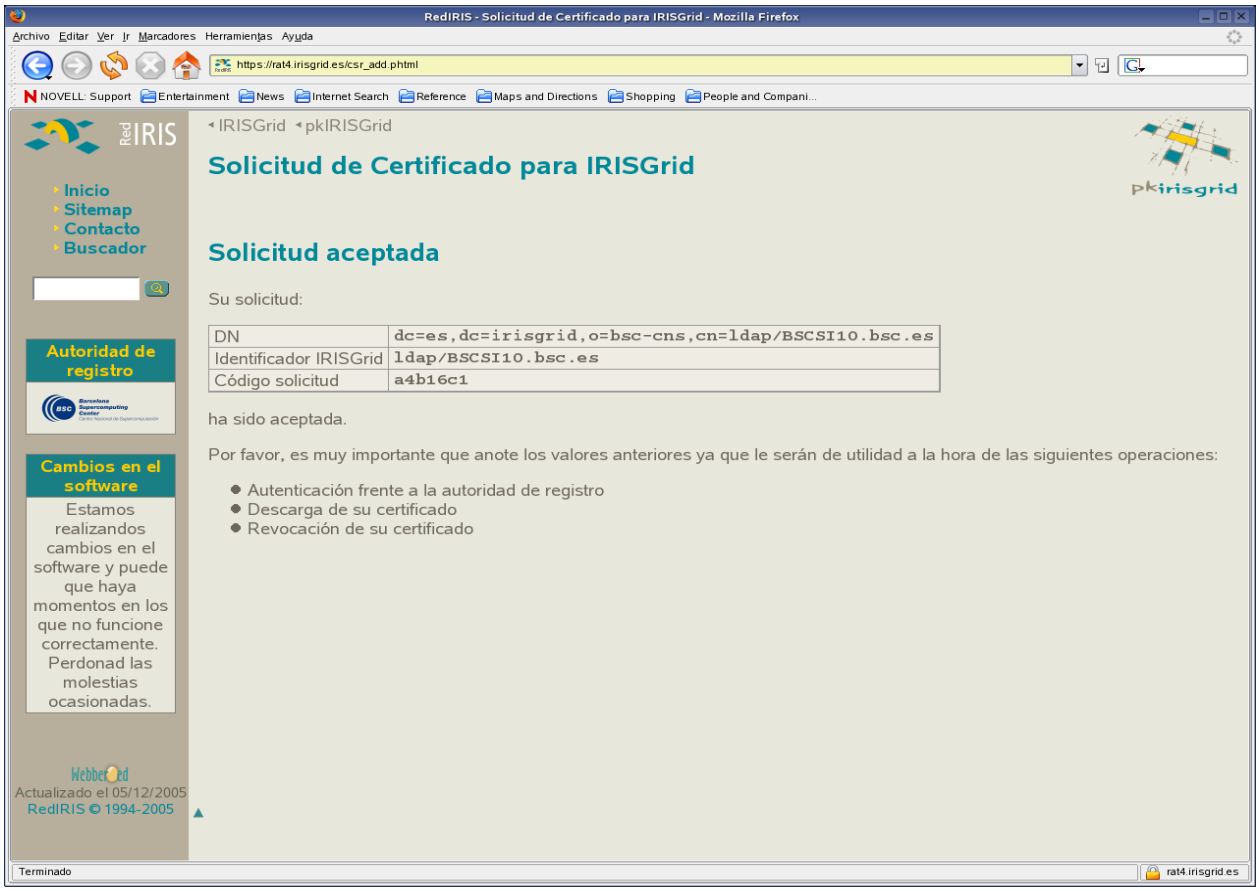


3 Must have the format: service/server name or server name; the domain must be chosen from the given list. The resulting host name must be a fully qualified domain name (FQDN); alias are not accepted.

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*.



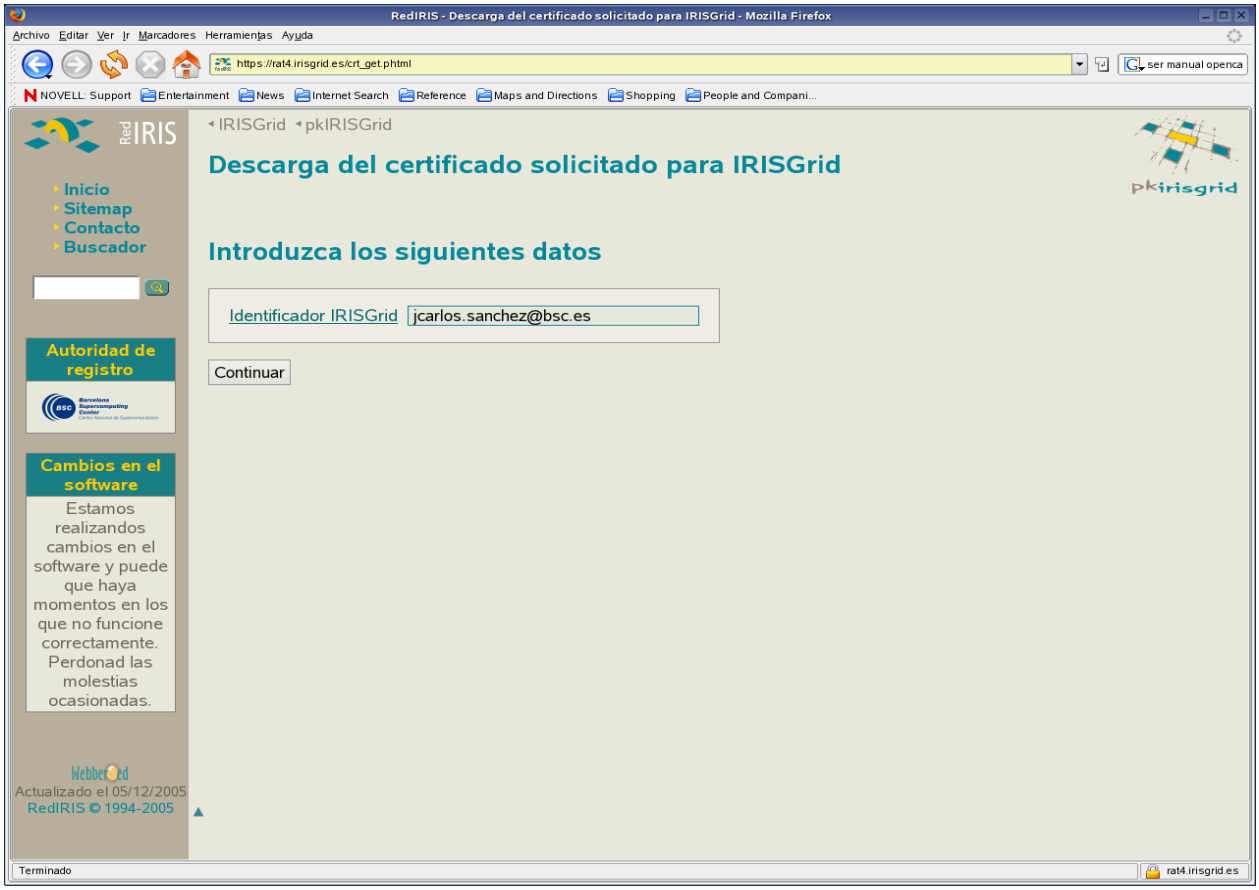
5. Validate your request certificate (see BSC-CNS RA Policy in section 1 of this document).

2.3 Get the signed certificate

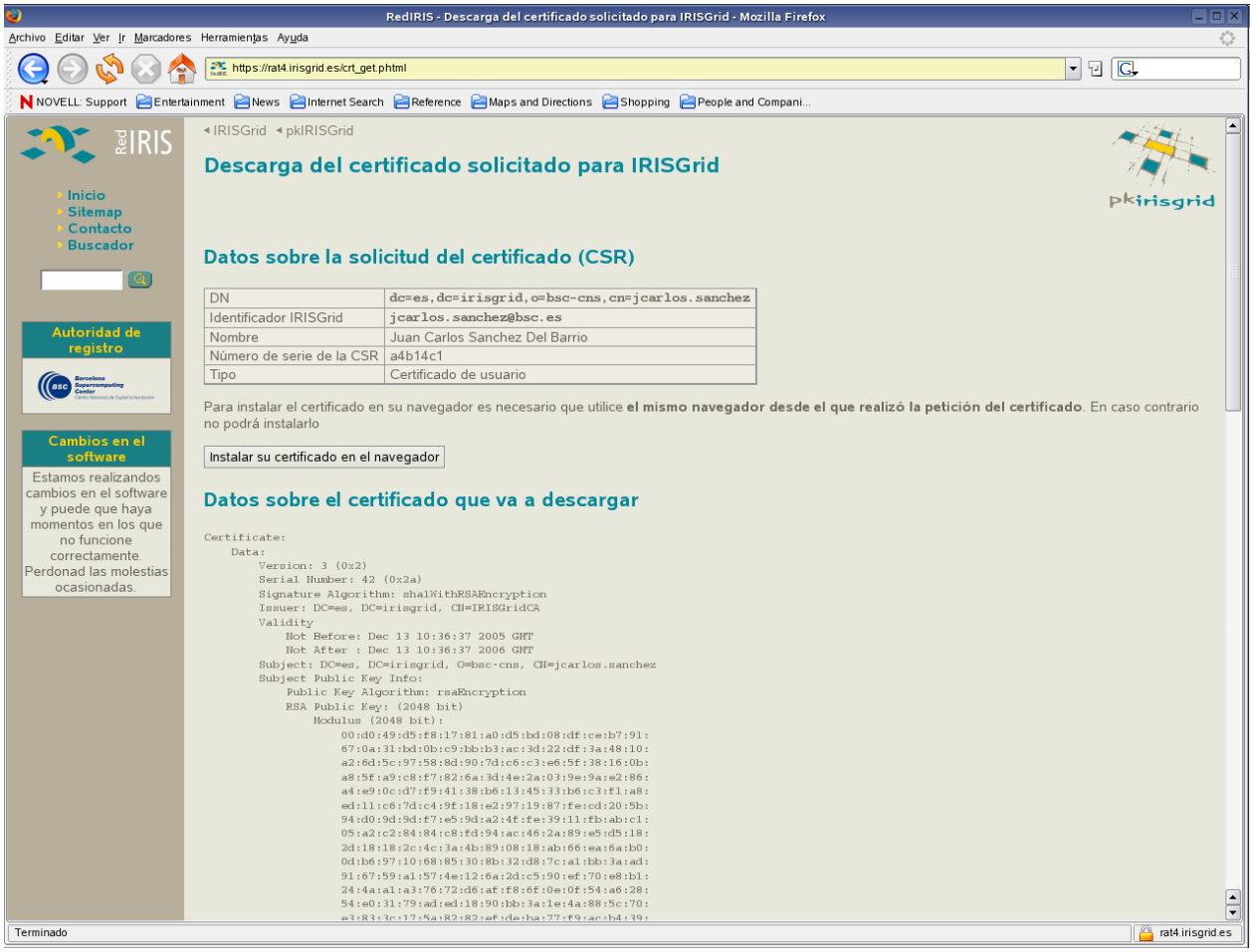
The signed certificate must be retrieved from the same web browser (in the same computer) used to issue the certificate request (CSR). This is important because the web browser needs to link the certificate back to the CSR and private keys, and this can be done in the browser where the CSR was generated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

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

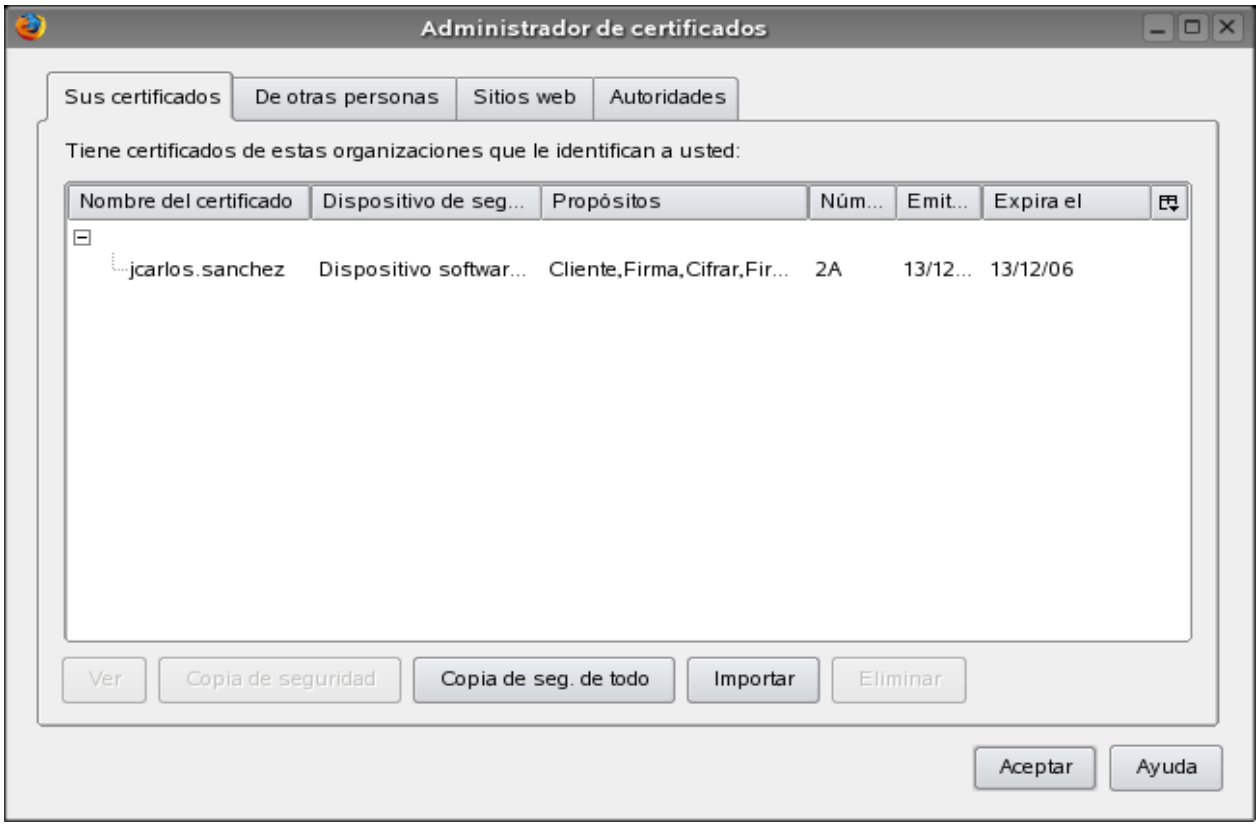
2. Introduce the corresponding "*Identificador IRISGrid*" and Click the "*Continuar*" button.



3. 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.



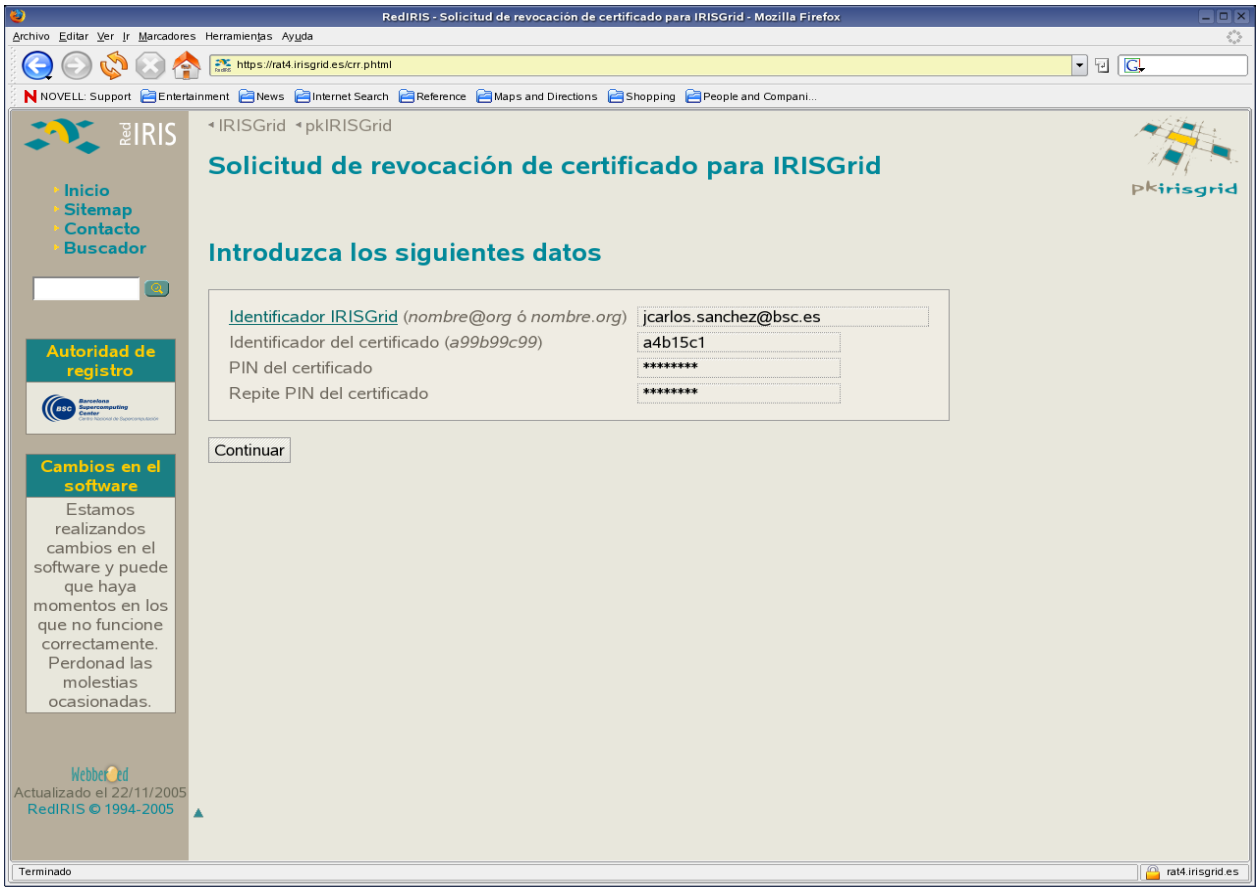
4. To verify that the certificate is installed correctly, Go to "*Editar-->Preferencias--> Avanzadas--> Certificados-->Administrador de Certificados-->Sus Certificados*" on the Mozilla Web Browser.



2.4 Revoke Certificate

1. Click on the "*Revocar Certificado*" link.

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.

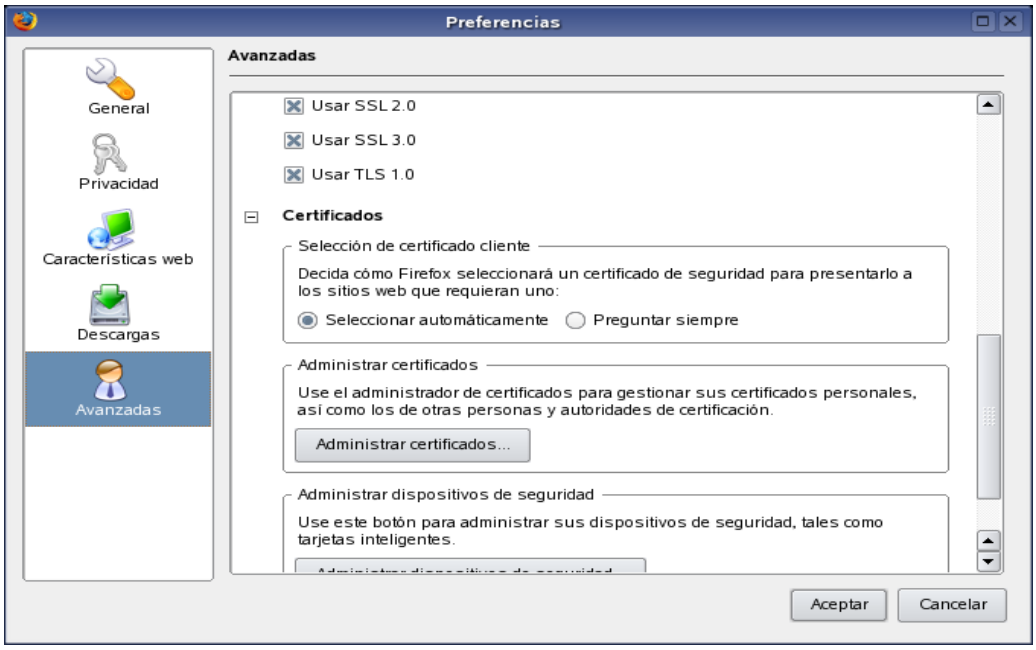


3. Click on the "*Solicitar la revocación*" button.

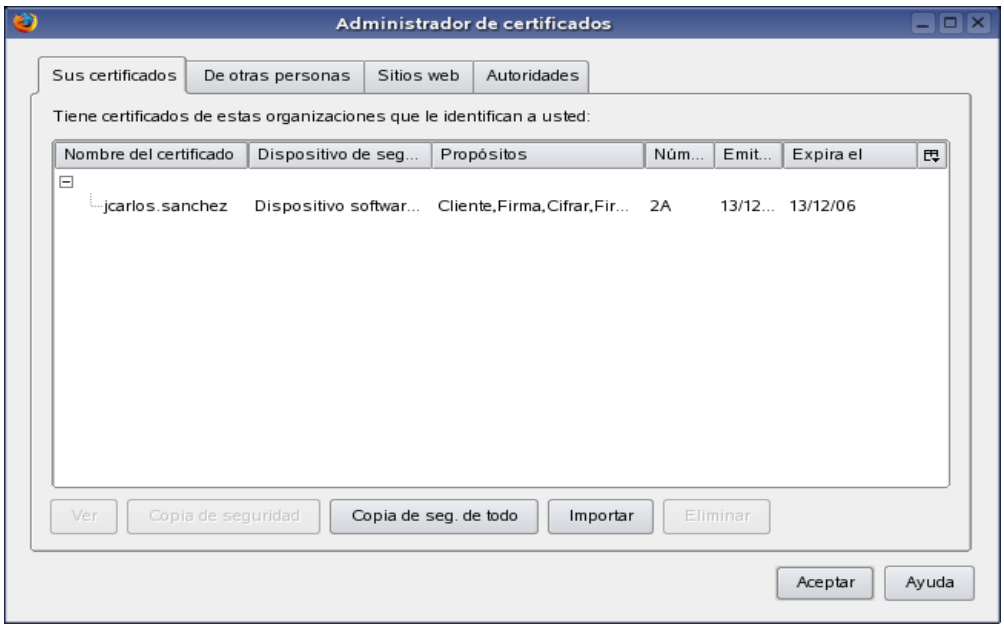
4. *pkIRISGrid* sends your revocation request to certificate revocation requests list (CRRL).

2.5 Export/Backup certificates

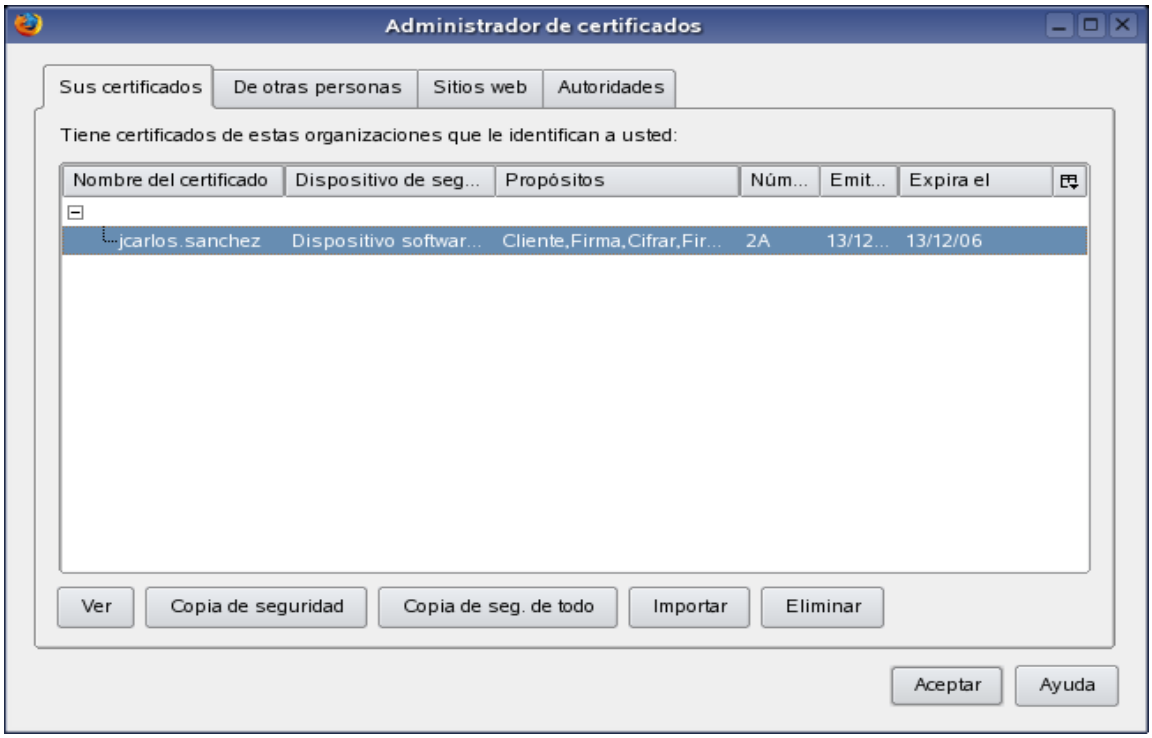
1. From the "*Editar*" menu select "*Preferencias*" and open the "*Avanzadas*" category and click on the "*Certificados*" item.



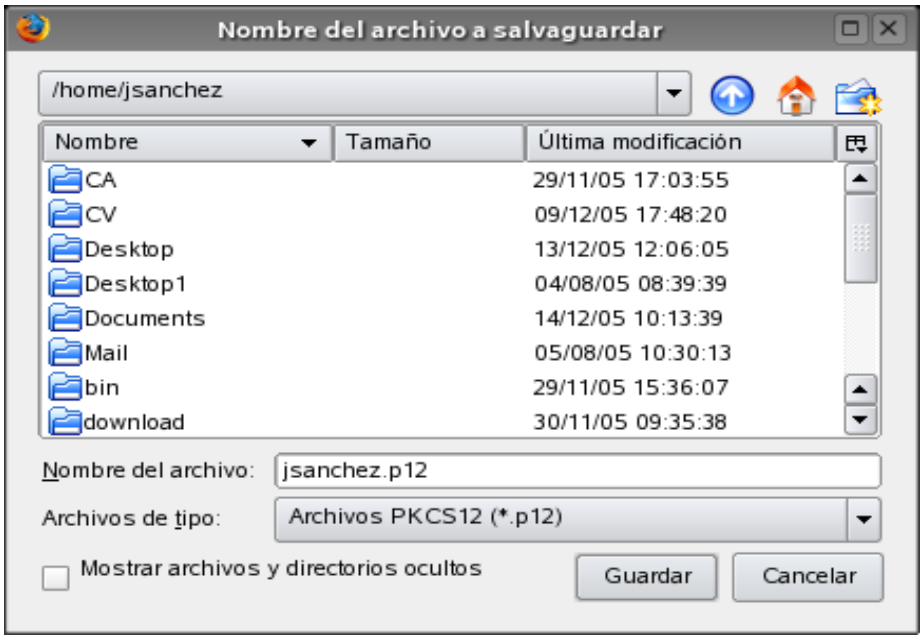
2. In the "*Administrador certificados*" section, click on the "*Administrar certificados...*" button. In the "*Administrador certificados*" window the "*Sus certificados*" tab should automatically open (if not, select it).



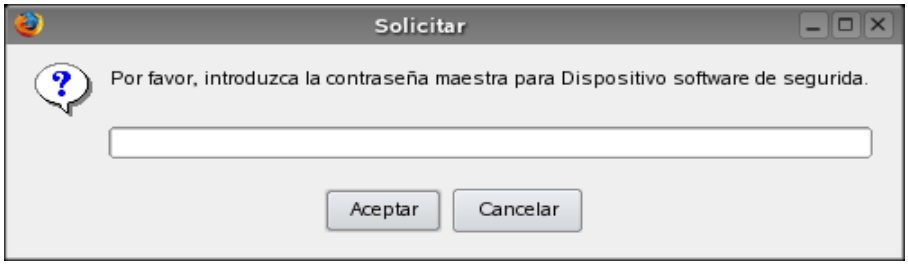
3. To export your personal certificate, click on it to select it, and click the "*Copia de seguridad*" button at the bottom of the window.



4. 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*".

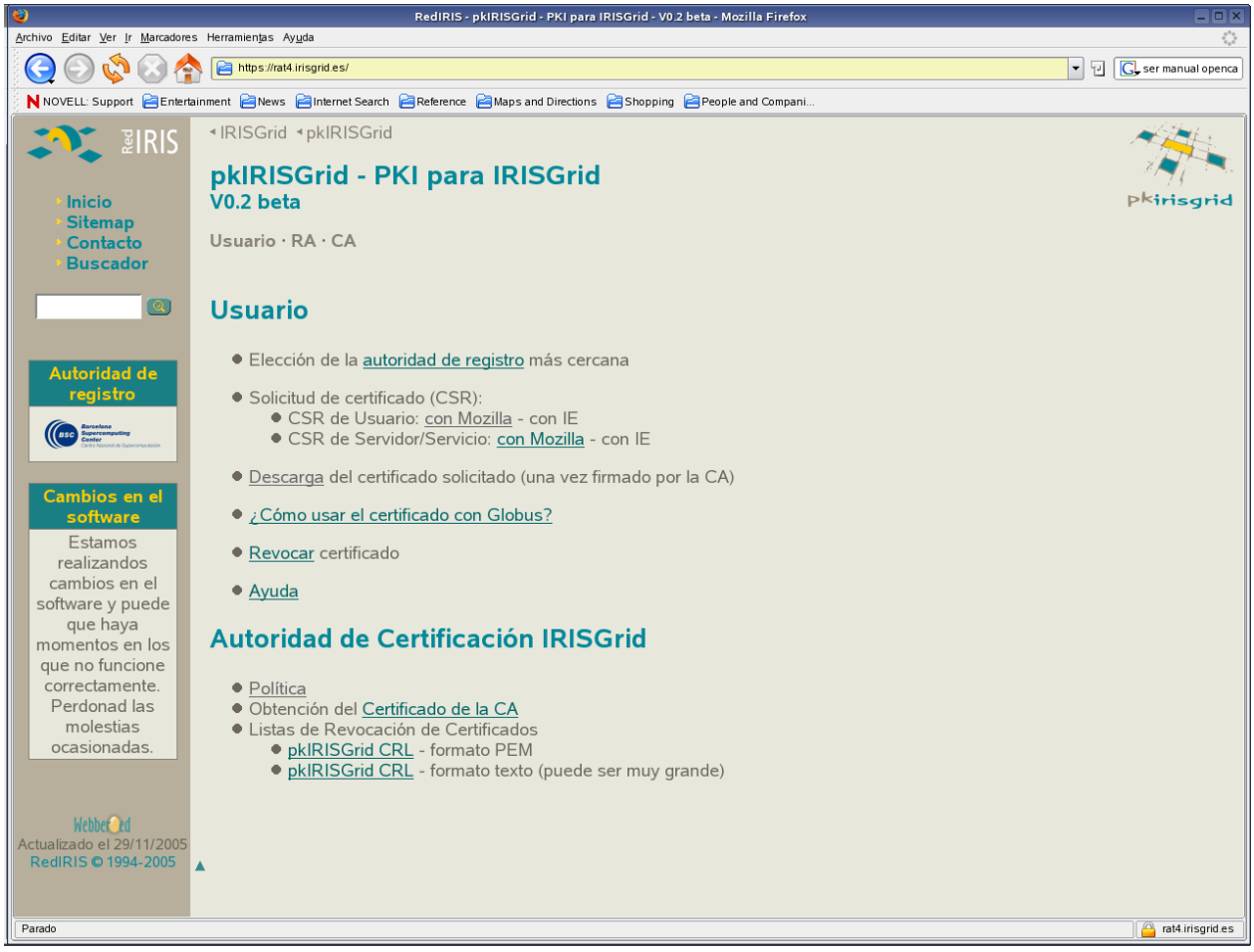
3 CA

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

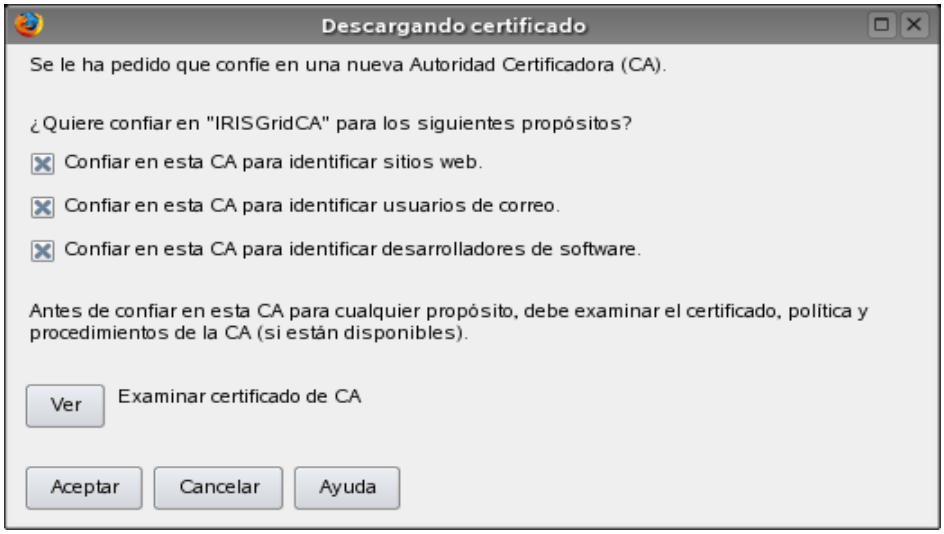
3.1 Get CA certificate

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

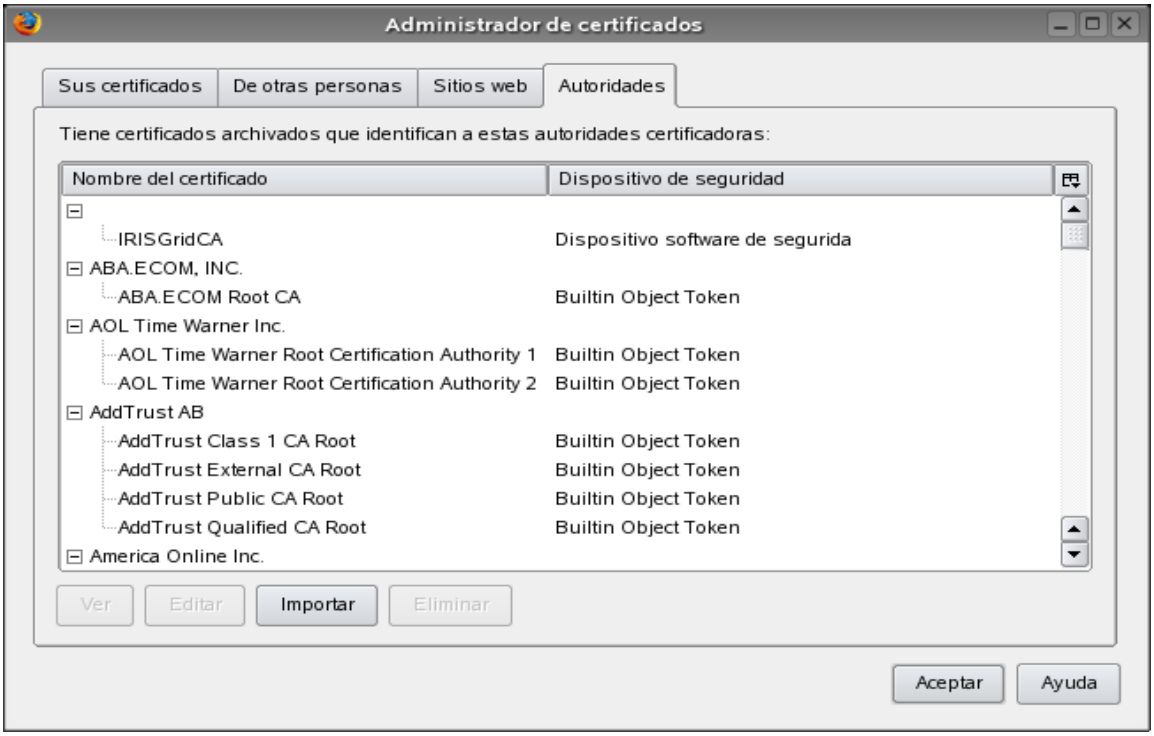
1. Click on the "*Obtención del Certificado de la CA*" link.



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/