Centro de Supercomputación de Galicia

Guía de usuario para la RA CESGA

v.: 2.2

Santiago de Compostela, 26 de abril de 2010

Historia

Version	Fecha	Comentario	Autor
0-1	24/11/2008	Redacción del documento	Esteban Freire (CESGA)
1-0	26/11/2008	Actualizado con la revision/comentarios	Alvaro Simon (CESGA)
1-1	02/12/2008	Actualizado con la revision/comentarios	Sergio Díaz (CESGA)
2-0	08/06/2009	Actualizado con la revision/comentarios	Javier López (CESGA)
2-1	12/06/2009	Actualizado con la última revisión de la política para la RA CESGA	Esteban Freire (CESGA)
2-2	09/04/10	Revisión y actualización de la guía de usuario	Esteban Freire (CESGA)

Índice de contenido

1. PRESENTACIÓN

En el presente documento se detalla la guía de usuario que explica como solicitar, renovar o revocar un certificado digital para una persona física o para un servidor/servicio bajo el Centro de Supercomputación de Galicia (en adelante CESGA) como RA de pkIRISGrid. También se explica como usar el certificado con Globus y como cambiar el responsable para un servidor/servicio El papel del CESGA como RA de pkIRISGrid es validar la autenticación de los usuarios que soliciten certificados de usuario o servidor bajo el dominio **cesga.es.**

El CESGA, situado en Santiago de Compostela, es el centro de cálculo, comunicaciones de altas prestaciones y servicios avanzados de la Comunidad Científica Gallega, sistema académico universitario y del Consejo Superior de Investigaciones Científicas (CSIC).

2. SOLICITUD DE CERTIFICADO:

Para obtener un certificado deberá descargar el documento con la política y los formularios de solicitud para la RA del CESGA desde el siguiente enlace:

http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf

Después de **haber leído el documento,** deberá acceder a la página, https://pk.irisgrid.es/rat8/. En el apartado **"Solicitud de certificado (CSR)"** hay dos opciones, "**CSR de Usuario"** y "**CSR de Servidor/Servicio"**, según se solicite un certificado digital de usuario o servidor respectivamente. Según la solicitud de certificado elegida, pulse sobre *Mozilla* o *IE*, conforme al navegador de Internet usado para solicitar el certificado. En el caso de los ejemplos contenidos en esta guía, el navegador usado es Mozilla. Firefox.

A continuación vamos a explicar el significado de los campos más importantes que se deben cubrir a la hora de solicitar un certificado digital. Luego se explicará como solicitar un certificado digital para usuario y para servidor.

2.1. INFORMACIÓN SOBRE LOS CAMPOS MÁS IMPORTANTES A CUBRIR A LA HORA DE SOLICITAR UN CERTIFICADO DIGITAL DE USUARIO O SERVIDOR:

- Identificador IRISGrid

  Es el identificador que identifica a una persona o a un servicio/servidor dentro de IRISGrid.

  - En el caso de un certificado digital de usuario:

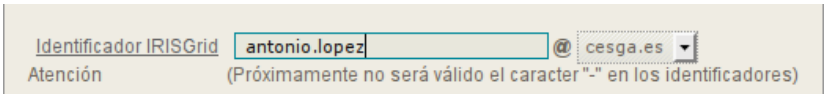
    Se recomienda encarecidamente utilizar como identificador IRISGRID:

    [nombre + separador + apellido].

    - Ejemplos válidos:

      antonio.lopez@cesga.es

      antoniolopez@cesga.es



- En el caso de un certificado digital de servidor:

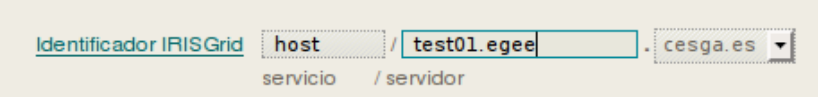
  En el campo servicio, se deberá introducir la palabra **host**, en el campo servidor, el nombre de la máquina, y dejar el dominio **cesga.es.**

  - Ejemplos válidos:

    host/test.cesga.es

    host/test.subdominio.cesga.es

    host/test.server.subdominio.cesga.es



- Clave de usuario

  Clave que sólo servirá para verificar la identidad de la persona que solicita el certificado ante una petición de la RA CESGA, se pedirá únicamente para validar que el usuario es quien solicitó el certificado a la hora de aprobar la solicitud.

- PIN para certificado

  Esta contraseña nos servirá para que en solicitudes futuras a la RA podamos confirmar que realmente nos pertenece el identificador de nuestro certificado, de modo que en el caso de que el certificado haya caducado y otra persona intente solicitar un certificado con el mismo identificador no podrá ya que no posee nuestro PIN.

  No se usa ni para exportar el certificado ni para usarlo con Globus.

  Ambas contraseñas "Clave de usuario" y "PIN para certificado" deben ser guardadas por el usuario cuando solicita el certificado.

- Privacidad. Publicación del e-mail en el certificado. Está opción esta disponible sólo para certificados de usuario

  Por defecto está opción esta marcada como **"No"**, y es recomendable dejarla por defecto. En caso de marcar **"Si"**, estamos haciendo pública nuestra dirección de correo electrónico en el interior del certificado

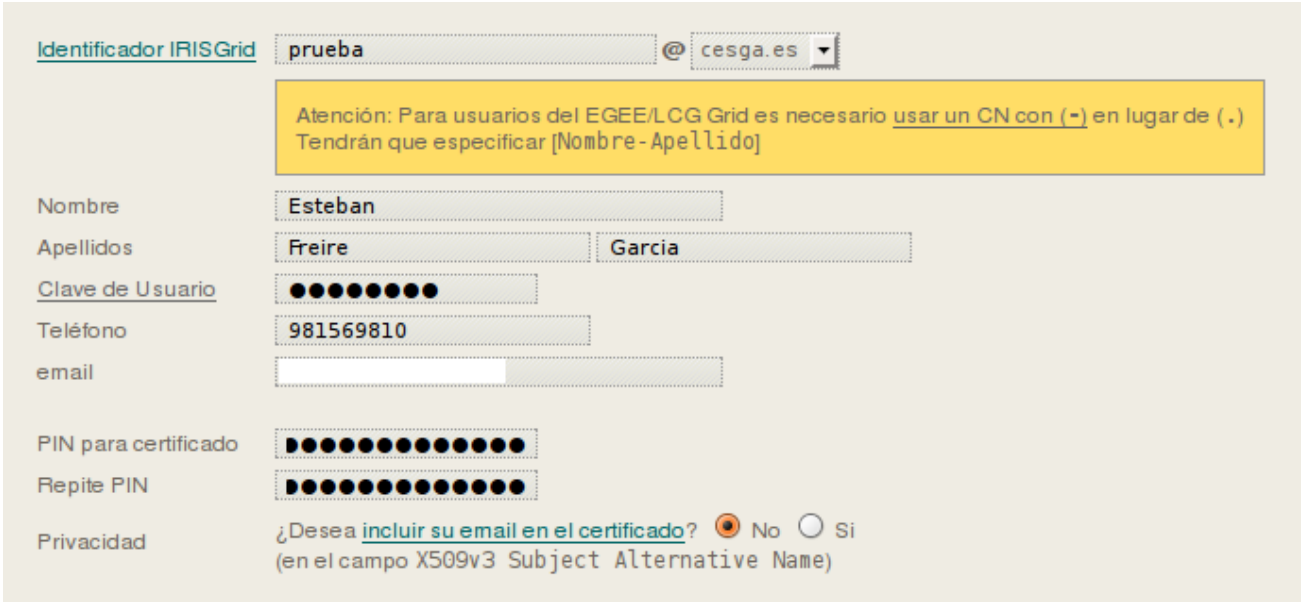
2.2. SOLICITUD DE CERTIFICADO DE USUARIO:

Como se ha dicho en el apartado *2. Solicitud de certificado*, antes de cubrir el formulario de solicitud se debe leer el documento con la política para la RA CESGA,

http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf.

También es recomandable rellenar el formulario de solicitud de certificado en la página, https://pk.irisgrid.es/rat8/ al mismo tiempo que cubre el formulario de solicitud de certificado de usuario que viene en el documento con la política.

Después de haber pulsado sobre el navegador usado en la opción, "**CSR de Usuario"**, se deberán cubrir los campos que aparecen para la solicitud de certificado. Ejemplo:



Una vez que se hayan cubierto todos los campos, pulse sobre el botón "Continuar". Aparecerá otra pantalla en la que se debe elegir el tamaño de la clave. Para este paso, ir al apartado 2.4. *SELECCIONAR EL TAMAÑO DE LA CLAVE.*

2.3. SOLICITUD DE CERTIFICADO DE SERVIDOR/SERVICIO:

Como se ha dicho en el apartado *2. Solicitud de certificado*, antes de cubrir el formulario de solicitud se debe leer el documento con la política para la RA CESGA,

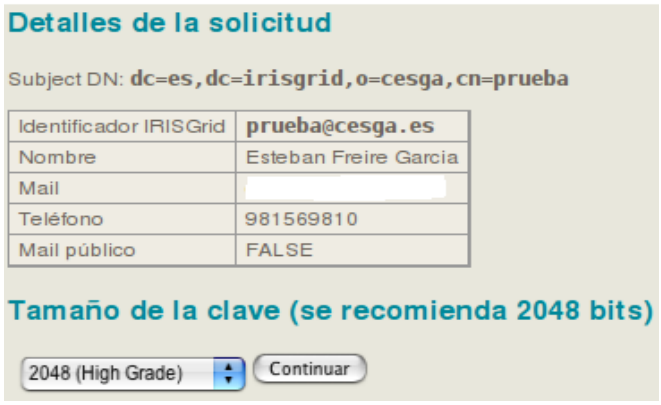
http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf. También es recomandable rellenar el formulario de solicitud de certificado en la página, https://pk.irisgrid.es/rat8/ al mismo tiempo que cubre el formulario de solicitud de certificado de servidor que viene en el documento con la política.

Después de haber pulsado sobre el navegador elegido en la opción, **CSR de Servidor/Servicio**, se deberán cubrir los campos que aparecen para la solicitud de certificado. Ejemplo:

Una vez que se hayan cubierto todos los campos, pulse sobre el botón “Continuar”. Aparecerá otra pantalla en la que se debe elegir el tamaño de la clave. Para este paso, ir al apartado 2.4. *SELECCIONAR EL TAMAÑO DE LA CLAVE.*

2.4. SELECCIONAR EL TAMAÑO DE LA CLAVE

Cuando hayamos rellenado todos los datos, pulsamos el botón continuar, lo que nos llevará a la generación de la CSR (de forma automática) por el navegador web. Se recomienda que el tamaño de la clave privada sea 2048 bits, aunque este valor se puede modifica.



Una vez seleccionado el tamaño de la clave pulse en el botón “Continuar” para completar el proceso de solicitud y enviar el certificado a la RA CESGA. Con el fin de que el proceso de autenticación se pueda completar, después de haber enviado el certificado a la RA CESGA, **un operador de la RA se pondrá en contacto con la persona que ha solicitado el certificado para concertar una reunión personal en el CESGA,** en dicha reunión se procederá a comprobar que el formulario de solicitud de certificado esté debidamente cubierto y a la autenticación de la persona que solicita el certificado que debe presentar uno de los documentos aceptados de acuerdo a la política de la RA CESGA,

http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf

También se verificará la clave de usuario, la cual fue introducida al solicitar el certificado.

En el plazo de unos días, una vez verificada la solicitud, recibirá un correo indicando que su certificado ha sido firmado y que esta disponible para descargar. Ejemplo:

2.5. DESCARGA DEL CERTIFICADO SOLICITADO

Desde el mismo navegador que se solicitó el certificado digital de usuario o servidor, se debe ir a la página de pkIRISGrid, https://pk.irisgrid.es/rat8/crt_get.phtml, para poder descargar el certificado.

Al acceder a este enlace, se deberá introducir el **“Identificador IRISGrid”** de nuestro certificado**.**

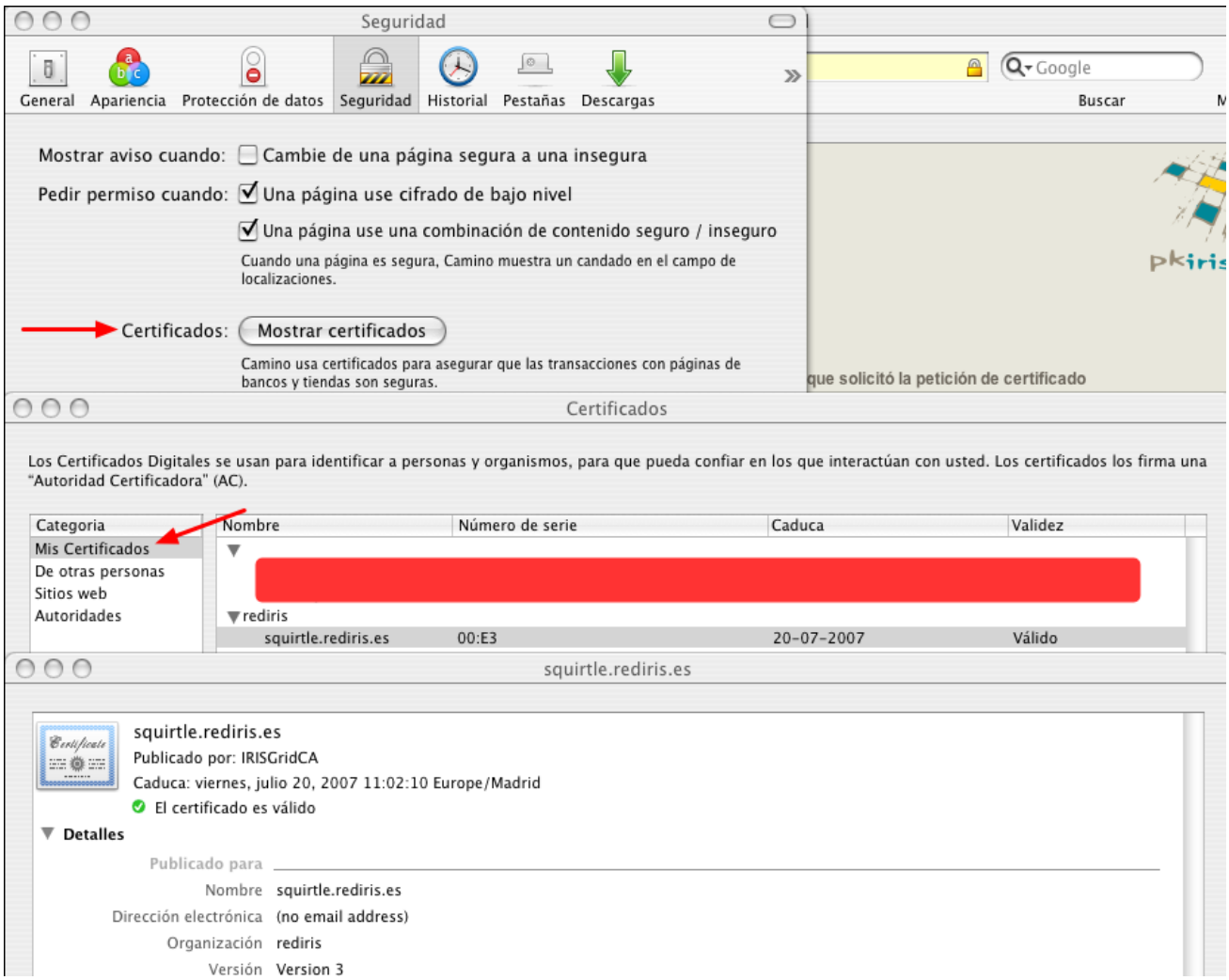
El identificador para el certificado es indicado en el correo que se envía desde pkIRISGrid indicando que el certificado está disponible para su descarga, como se puede ver en el anterior ejemplo.

Una vez introducido el identificador del certificado:

Pulse sobre el botón "Continuar", aparecerá una ventana con los datos sobre la solicitud del certificado, también aparece una advertencia que nos dice que sólo podemos descargar el certificado si usamos el mismo navegdor desde el que realizamos la solicitud. Esto de debe a que es el navegador web quien tiene la clave privada de dicho certificado, y por tanto es el único capaz de descargarl

Pulse en "**Instalar su certificado en el navegador",** el navegador web nos pedirá la "master password for the Security Software Device", si aún no la hemos introducido. Una vez introducida esta contraseña (que es propia del navegador web), el certificado será descargado.

Para comprobar que el certificado se ha descargado correctamente, abrimos las preferencias del navegador; y en concreto la gestión de certificados. (Esto puede variar de unas versiones a otras de los navegadores, pero la idea es la misma en todos ellos). Hacemos que el navegador nos muestre los certificados, en concreto Mis Certificados. Y comprobamos que esté ahí el certificado que acabamos de instalar en el navegador:



Puede ser encontrada más información sobre como solicitar y descargar un certificado digital en el siguiente enlace,http://www.irisgrid.es/pki/doc/serverCertReq.phtml

3. EXPORTAR EL CERTIFICADO CON FORMATO PKCS#12 PARA PODER SER USADO CON GLOBUS

Para poder usar el certificado con Globus, es necesario exportar el certificado y la clave privada. Los siguientes ejemplos mostrarán como extraer el certificado y la clave en formato PKCS#12, que suele guardarse en un fichero con extensión **.p12**.

Para poder solicitar el certificado deberá acceder al gestor de certificados. Se puede dar uno de los siguientes casos:

- Navegador Mozilla/Firefox:
  - Ir a **"Herramientas"** – **"Opciones"** o en **“Editar”** - **“Preferencias”** (dependiendo de la versión del navegador)
  - Seleccionar el icono **"Avanzado"** y la pestaña “**Cifrado”**
  - Pulse el botón **"Ver certificados"**
  - Elija su certificado y pulse sobre el botón "**Hacer copia...**"

- Introduzca un nombre para el fichero y una ubicación, por ejemplo, *my_cert.p12*
- Introduzca la clave para acceder al servicio de seguridad del navegador (el sitio donde el navegador guarda internamente las claves)
- Introduzca una clave para proteger el fichero de copia del certificado

  Esta clave es la que se usará para las operaciones con Globus

- El certificado ha sido generado en la ubicación indicada

- Navegador Internet Explorer:
  1. Ir a **"Herramientas" - "Opciones de Internet" - "Contenido" - "Certificados"** – **"Pestaña Personal"**
  2. Seleccione el certificado de IRISGrid
  3. Seleccionar **"Exportar"**
  4. Seleccionar la opción: **Exportar la clave privada".**
  5. Seleccionar: **"Usar seguridad fuerte"**
  6. De seleccionar la opción: "**Borrar la clave privada después de exportar"**
  7. Introducir una clave para proteger el fichero de copia del certificado
     Esta clave es la que se usará para las operaciones con Globus
  8. Elija un nombre para el fichero, por ejemplo *my-cert-backup*. Será creado el fichero con un extensión .pfx
  9. El certificado ha sido generado en la ubicación indicada

3.1. EXTRAER LA CLAVE PRIVADA

Pasar el formato PKCS12 a formato PEM para poder usarlo con Globus, esto se puede hacer con los siguientes comandos **(reemplace my_cert.p12 o my_cert.pfx por el nombre de su fichero exportado)**:

- En el caso de un certificado de usuario:

```
> openssl pkcs12 -nocerts -in my_cert.p12 -out userkey.pem
> openssl pkcs12 -clcerts -nokeys -in my_cert.p12 -out usercert.pem
```

- En el caso de un certificado de servidor (no se encripta la clave privada):

```
> openssl pkcs12 -nocerts -nodes -in my_cert.p12 -out hostkey.pem
> openssl pkcs12 -clcerts -nokeys -in my_cert.p12 -out hostcert.pem
```

- Nota: En ambos casos el comando ejecutado pedirá una contraseña, esta contraseña es la que se tecleo para proteger el fichero de copia cuando exportó el certificado digital a formato PKCS12 o PFX.

Asegúrese de que los certificados tengan los permisos correctos:

```
> chmod 0400 userkey.pem
> chmod 0444 usercert.pem
```

Una vez generados los certificados, la ubicación recomendada y por defecto de los mismos es la siguiente:

- Ubicación para los certificados de host:

> /etc/grid-security/hostcert.pem (r-- r-- r--)

> /etc/grid-security/hostkey.pem (r-- --- ---)

- Ubicación para los certificados de usuario:

>$HOME/.globus/usercert.pem (r-- r-- r--)

>$HOME/.globus/userkey.pem (r-- --- ---)

- Donde el directorio $HOME/.globus es un directorio creado por el usuario (mkdir **$HOME/.globus**)

Puede ser encontrada más información sobre como usar el certificado con Globus y como extraer la clave privada en el siguiente enlace, https://pk.irisgrid.es/rat1/cert2globus.phtml#p12

4. CAMBIO DE RESPONSABLE DE UN CERTIFICADO DE SERVIDOR

En caso de que el administrador del servidor pase a ser una persona distinta será necesario que el nuevo responsable cubra el formulario de solicitud de certificado de servidor que viene en la política para la RA CESGA, http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf, para después presentarlo en una reunion personal con uno de los operadores de la RA CESGA. La reunión personal se puede concertar enviando un e-mail a la dirección de correo,

egee-admin@cesga.es

5. RENOVAR EL CERTIFICADO

Es necesario tener el certificado válido de pkIRISGrid que se desea renovar instalado en el navegador usado para hacer la renovación, tanto para renovaciones de certificado de usuario como de servidor, es decir, para renovar por ejemplo el certificado de un servidor es necesario tener cargado el certificado de este servidor en el navegador usado para hacer la renovación. Sólo se puede hacer la renovación durante los 30 días anteriores a la expiración del certificado, aunque se recomienda hacerla antes de los dos últimos días a la fecha de expiración del certificado.

Desde pkIRISGrid son enviados dos correos a la dirección e-mail indicada cuando se solicitó el certificado digital, el primero se envía cuando faltan 30 días para que expire el certificado y el segundo cuando faltan 7 días para que expire el certificado. Este e-mail informativo contiene los datos necesarios para renovar al certificado:

- DN del certificado
- Identificador IRISGrid
- Identificador certificado

Ejemplo:

Subject: pkIRISGrid - Su certificado >a8b9c3< expirara en 30 dXas
From: pkIRISGrid-CA
Date: 10/05/09 00:10
To: esfreire@cesga.es
content-transfer-encoding: quoted-printable

Su certificado cuyos datos se muestran a continuación expira en 30 días

Los datos de su certificado son:

DN del certificado: dc=es,dc=irisgrid,o=cesga,cn=[redacted]
Identificador IRISGrid: [redacted]@cesga.es
Identificador certificado: a8b9c3
Fecha de expiración: 09/06/2009

Si ya solicitó la renovación del certificado no haga caso de este mensaje.

Un saludo

---

pkIRISGrid CA Team — Tel: +34 95 505 66 23
Red.ES/RedIRIS — Fax: +34 95 505 66 27
Edificio CICA. Avenida Reina Mercedes, s/n — http://www.rediris.es

En estos momentos, de acuerdo a la política para la RA del CESGA,

http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf, no es necesario cubrir ningún formulario a la hora de solicitar la renovación del certificado.

Para renovar el certificado con la RA del CESGA se deberá acceder a la página, https://pk.irisgrid.es/rat8/, una vez allí pulse sobre la opción "Renovar certificado", en la siguiente ventana se deben introducir los datos necesarios para renovar al certificado (comentados al principio de este apartado).

Se debe introducir el **"Identificador IRISGrid"** del certificado (por ejemplo, *antonio-lopez@cesga.es*, o por ejemplo, *host/test.subdominio.cesga.es*, en el caso de un certificado de servidor), el **"Identificador del certificado"** (por ejemplo, *099b99c99)* y por último el PIN del certificado. Una vez introducidos estos datos, pulse en el botón "Continuar", en la siguiente ventana aparecen los datos del certificado, pulse en el botón **"Solicitar la renovación"**. Como ya se ha dicho anteriormente, los datos necesarios para solicitar la renovación son enviados en el correo desde pkIRISGrid informando de la expiración del certificado.

A continuación desde la RA del CESGA, se procederá a verificar la renovación y en el plazo de uno o dos días, el solicitante debería recibir un e-mail informando que el certificado puede ser descargado. A partir de aquí se pueden seguir los pasos descritos en el apartado 3. *DESCARGA DEL CERTIFICADO SOLICITADO.*

Ejemplo:

6. REVOCAR EL CERTIFICADO

Es necesario tener el certificado válido de pkIRISGrid que se desea revocar instalado en el navegador, tanto para revocaciones de certificado de usuario como de servidor, es decir, para revocar por ejemplo el certificado de un servidor es necesario tener cargado el certificado de este servidor en el navegador usado para hacer la revocación.

Tanto para revocar certificados de usuario como certificados de servidor, de acuerdo a la política para la RA del CESGA, http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf, es necesario cubrir uno de los siguientes formularios incluidos en el documento con la política, *"SOLICITUD DE REVOCACIÓN DE CERTIFICADO DE USUARIO POR INICIATIVA DEL USUARIO"* o *"SOLICITUD DE REVOCACIÓN DE CERTIFICADO DE SERVIDOR POR INICIATIVA DEL USUARIO"*, respectivamente.

Para revocar el certificado es necesario acceder a la página, https://pk.irisgrid.es/rat8/, y hacer doble clic en la opción **"Revocar certificado",** en la siguiente ventana, se debe introducir el **"Identificador IRISGrid"** del certificado (por ejemplo, *antonio-lopez@cesga.es*, o por ejemplo, *host/test.subdominio.cesga.es*, en el caso de un certificado de servidor), el "I**dentificador del certificado"** (por ejemplo, *099b99c99)* y por último el PIN del certificado. Ejemplo:

Una vez introducidos estos datos, pulse sobre el botón **“Continuar con la REVOCACION”**, en la siguiente ventana aparecen los datos del certificado, pulse sobre el botón **“Solicitar la revocación”.**

Una vez solicitada la revocación, un operador de la RA se pondrá en contacto con la persona que ha hecho la solicitud para concertar una reunión personal en el CESGA, en dicha reunión se procederá a comprobar que el formulario de solicitud de revocación de certificado está debidamente cubierto, y a la autenticación de la persona que solicita revocar el certificad, que debe presentar uno de los documentos aceptados de acuerdo a la política de la RA CESGA,

http://www.irisgrid.es/pki/policy/ra/pkirisgrid-cesga-policy-2.2.0-20100409.pdf. También se verificará la clave de usuario, la cual fue introducida al solicitar el certificado. Una vez hecha la autenticación, un operador de la RA del CESGA procederá a revocar el certificado.