

# Centre d'Investigació en Nanociència i Nanotecnologia

## CIN2



# Política de la Autoridad de Registro (RA) CSIC-Bellaterra

## de pkIRISGrid

versión: 1.0.1

Bellaterra, 2 de Julio 2009

# Índice de contenido

<b>Política de la Autoridad de Registro CSIC-Bellaterra .....</b>	<b>3</b>
<b>Historia .....</b>	<b>3</b>
<b>1. Presentación .....</b>	<b>4</b>
<b>2. Operadores de la RA.....</b>	<b>4</b>
<b>3. Aprobación de solicitudes de certificado.....</b>	<b>4</b>
3.1. Autenticación del solicitante.....	4
3.1.1. Reunión cara a cara.....	4
3.1.1.1 Detalles de la reunión .....	5
3.1.1.2 Documentos de identificación aceptados.....	5
3.1.1.3. Documento acreditativo de vinculación laboral con los centros .....	5
3.1.1.4 Documentación archivada .....	5
3.1.2 Otros métodos .....	6
3.2 Verificación del solicitante.....	7
3.2.1 Descripción del procedimiento para certificado de personas físicas.....	7
3.2.1.1 Verificación en la reunión cara a cara .....	7
3.2.1.2 Descripción del procedimiento para certificado de servidor.....	7
3.2.1.3. Cambio de administrador para el servidor .....	7
3.2.3 Documentación archivada.....	7
<b>4. Política de revocaciones .....</b>	<b>8</b>
4.1 Solicitud de revocaciones por iniciativa de la RA.....	8
4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado.....	8
4.3 Solicitud de revocación cuando un usuario abandona la institución.....	8
<b>Anexo I - Solicitud de certificado de usuario pkIRISGrid.....</b>	<b>9</b>
<b>Anexo II - Solicitud de certificado de servidor pkIRISGrid.....</b>	<b>10</b>
<b>Anexo III - Revocación de certificado de usuario .....</b>	<b>11</b>
<b>Anexo IV - Revocación de certificado de servidor .....</b>	<b>12</b>

## Política de la Autoridad de Registro CSIC-Bellaterra

El "Centre d'Investigació en Nanociència i Nanotecnologia", en adelante el CIN2 presenta en éste documento la política de la Autoridad de Registro (RA) CSIC-Bellaterra.

### Historia

10/06/2009	0.0.1	Lino García Tarrés	Redacción.
11/06/2009	0.0.2	Lino García Tarrés	Cambio formularios revocación.
12/06/2009	0.0.3	Lino García Tarrés	Incorporación logotipo
16/06/2009	0.0.4	Javier Masa	Inclusión solicitante acepta la política de pkIRISGrid
17/06/2009	0.0.5	Lino García Tarrés	Autorización para la delegación de dominio icmab.es
17/06/2009	0.0.6	Javier Masa	Eliminación enlaces antiguos
01/07/2009	1.0.0	Victor Castelo	Cambio nombre RA por CSIC-Bellaterra
02/07/2009	1.0.1	Javier Masa	Cambio urls

## 1. Presentación

Situado en Bellaterra (Barcelona), el CIN2 es una institución dedicada a la investigación sobre Nanociencia y a las tecnologías que de ellas se derivan. Con ánimo de ser un referente internacional de excelencia científica, el CIN2 es un centro mixto formado por el Consejo Superior de Investigaciones Científicas (CSIC) y el “Institut Català de Nanotecnologia” (ICN).

El Institut de Ciencia de Materials de Barcelona (ICMAB) un centro de investigación del CSIC dedicado a la investigación dirigida a la obtención y a la caracterización de materiales de interés industrial. Sus actividades se centran en la síntesis, la preparación, la cristalización y la caracterización de los materiales y nanomateriales funcionales de altas prestaciones

En la actualidad trabajan entre ambos centros más de 200 investigadores que participan activamente en proyectos de eCiencia haciendo algunos de ellos uso de pkIRISGrid. La activa participación tanto de los investigadores locales como de los visitantes en la infraestructura GRID, hace necesaria la RA del CSIC-BELLATERRA, motivos por los cuales el CIN2 solicita y define ésta política.

## 2. Operadores de la RA

Los operadores de la RA del CSIC-Bellaterra deben tener contrato laboral con el CIN2, el ICMAB, el CSIC o el ICN, con más de dos años de experiencia y conocimientos medios de informática.

Todos los operadores de la RA CSIC-BELLATERRA deben haber sido formados para su labor por personal de pkIRISGrid o por otros operadores de la RA CSIC-Bellaterra.

La contraseña se cambiará en el momento en que un operador deja de serlo o abandona el CIN2, el CSIC el ICMAB o el ICN, y deberá ser comunicada al resto de operadores.

## 3. Aprobación de solicitudes de certificado.

La RA CSIC-Bellaterra aprueba solicitudes de certificado tanto de usuario como de servidor para sus investigadores.

La RA también aprueba solicitudes de certificado, tanto de usuario como de servidor, siempre y cuando se soliciten para el dominio icmab.es y el solicitante tenga vinculación laboral con el ICMAB.

El usuario podrá solicitar desde su navegador, en el enlace para la RA CSIC-Bellaterra (<https://pki.irisgrid.es/rat38>), su certificado de usuario o certificados de servidor.

### 3.1. Autenticación del solicitante

El proceso de autenticación del solicitante de certificados será el mismo tanto para solicitudes de certificado de usuario como de servidor.

#### 3.1.1. Reunión cara a cara

La única forma de autenticación del solicitante de un certificado es mediante la **reunión cara a cara**.

Una vez solicitado el certificado y contactado por un operador de la RA, el solicitante deberá presentar en el CIN2 los siguientes documentos:

- Formulario de solicitud debidamente cumplimentado y firmado (Anexo I o Anexo II)
- Documento de identificación aceptado (3.1.1.2)

- Documento acreditativo de vinculación laboral con algunos de los centros (3.1.1.3)

El solicitante, deberá comunicar el PIN de la solicitud al operador, y éste procederá a generar la documentación descrita en el punto 3.1.1.4, archivarla, y aprobar la solicitud si procede.

Una vez aprobada, el operador de la RA enviará la solicitud a la CA en el plazo de dos días laborables.

#### 3.1.1.1 Detalles de la reunión

La RA CSIC-Bellaterra está situada en la sede central del instituto CIN2 (Edificio Q (ETSE) – piso 2º. Campus UAB. 08193 Bellaterra). El horario de apertura se indicará en la web del mismo. El solicitante dispondrá de un plazo de 7 días hábiles para acudir a la reunión cara a cara después de que el operador de la RA haya contactado con él, si bien los días pueden variar dependiendo de la disponibilidad de los operadores.

#### 3.1.1.2 Documentos de identificación aceptados

Los documentos aceptados para la identificación del solicitante del certificado de usuario o de servidor son los siguientes:

- Ciudadanos españoles: **DNI** (tradicional, electrónico), **pasaporte** o permiso de **conducir**.

Ni el carné del CIN2 ni cualquier otro documento similar será aceptado para la autenticación aunque tengan fotografía.

En el caso de uso del DNI electrónico deberá mostrarse en la reunión cara a cara al operador de la RA. No será válido el envío de un correo electrónico firmado con el certificado incluido en el DNI electrónico para evitar la reunión cara a cara.

- Ciudadanos comunitarios: **Pasaporte** o bien el documento de **identidad legal en su país** de origen, siempre que contenga fotografía.
- Ciudadanos extranjeros: **Pasaporte** o **NIE** (carné de Número de Identificación de Extranjeros). No se aceptarán NIE en tramitación, sólo definitivos con la tarjeta que muestre la fotografía

#### 3.1.1.3. Documento acreditativo de vinculación laboral con los centros

El solicitante debe acreditar su vinculación laboral con uno de los siguientes centros:

- “Centre d’Investigació en Nanociència i Nanotecnologia” (CIN2).
- “Institut de Ciència de Materials de Barcelona” (ICMAB).

Para ello será necesario presentar un certificado emitido por la Gerencia de su centro en el que se especifique el periodo de vinculación laboral.

En caso de que el solicitante sea personal visitante del CIN2 o del ICMAB, deberá presentar un documento, firmado por el director de la institución correspondiente, que le acredite como tal.

#### 3.1.1.4 Documentación archivada

En el proceso de autenticación del solicitante el operador de la RA contrastará los datos de la solicitud del certificado con los del documento de identidad presentado. Si los datos son correctos, se fotocopiarán tanto el documento de identidad presentado como el documento con los datos de la solicitud de certificado que el usuario imprimió al realizar la misma y el documento acreditativo de vinculación laboral con el centro, y se guardarán para futuras auditorias.

### **3.1.2 Otros métodos**

No aplicable.

## **3.2 Verificación del solicitante**

Tras la autenticación del solicitante, se ha de verificar la autoridad de éste antes de aprobar la solicitud. La verificación se hará mediante el formulario de solicitud, comprobando que el formulario este debidamente cubierto, firmado y sellado. En todos los casos se verificará que la dirección de correo electrónico que aparece en el formulario es la misma que se ha utilizado para pedir el certificado.

### **3.2.1 Descripción del procedimiento para certificado de personas físicas**

#### **3.2.1.1 Verificación en la reunión cara a cara**

El solicitante presentará en la reunión cara a cara con la RA uno de los documentos identificación del solicitante aceptados conforme el apartado 3.1.1.2 y el formulario solicitado en la fase de autenticación. El carné se fotocopiará y se guardará junto a las fotocopias de los documentos que se hicieron en la fase de autenticación.

La verificación se hará mediante el formulario de solicitud, comprobando que el formulario esté debidamente cumplimentado, firmado y sellado. Se verificará el correo electrónico pidiendo al solicitante que responda al correo con el que se le cita a la reunión cara a cara, antes de acudir a ella.

#### **3.2.1.2 Descripción del procedimiento para certificado de servidor**

El solicitante presentará en la reunión cara a cara con la RA uno de los documentos aceptados en el apartado 3.1.1.2 y el formulario solicitado en la fase de autenticación. Este formulario debe ser cubierto mientras solicita su certificado de servidor desde su navegador. La autenticación del solicitante se describe en los apartados 3.1.1 y 3.1.2.

La persona que solicita un certificado de servidor deberá presentar el formulario del Anexo II firmado por el responsable de la máquina y sellado por la institución a la que pertenece el solicitante, autorizando al solicitante a pedir un certificado de servidor, también se deberá indicar en el formulario la persona que administra el servidor. Si los datos son correctos, se fotocopiará el documento aceptado y se guardará con el formulario de solicitud presentado para futuras auditorías.

#### **3.2.1.3. Cambio de administrador para el servidor**

En caso de que el administrador del servidor pase a ser una persona distinta, será necesario que el solicitante vuelva a repetir el proceso que se describe en el apartado 3.2.1.2, pero no será necesario volver a solicitar el certificado desde la página de pkIRISGrid.

### **3.2.3 Documentación archivada**

Descrito en los apartados 3.2.1.1 y 3.2.1.2.

## 4. Política de revocaciones

Las siguientes subsecciones describen en qué casos la RA puede solicitar la revocación de un certificado. En todas las solicitudes de revocación se generará un informe con los datos del operador que la solicitó, la circunstancias que provocaron la solicitud, la fecha, y otros documentos justifiquen dicha decisión, como los datos de autenticación en caso de iniciativa del usuario, o informes que muestren el mal uso de los certificados.

### 4.1 Solicitud de revocaciones por iniciativa de la RA

La RA solicitará la revocación de un certificado por iniciativa propia cuando:

- En el caso de un usuario:
  - Está usando los servicios a los que tiene acceso con su certificado para usos ajenos al centro o de forma indebida.
  - Se detecta que el usuario tiene instalado el certificado en un ordenador al que tienen acceso varias personas.
  - Se detecta un robo de la clave pública.
  - El usuario comparte su certificado o le da otros usos incompatibles con el objetivo de un certificado digital.
  - El usuario deja de tener permiso de la institución que lo avaló para usar el certificado.
  - Otros usos del certificado que el operador estime incorrectos o que puedan dañar la imagen o la reputación de pkIRISGrid o del centro.
- En el caso de certificados de servicio/servidor:
  - Se detecta que la clave privada del servidor se ha visto comprometida.
  - Se detecta que el certificado está instalado en varias máquinas, sin ser un sistema de alta disponibilidad.
  - El servicio que ofrecía el servidor para el que se pidió el certificado deja de ofrecerse.

### 4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado

La RA solicitará la revocación de un certificado a petición del usuario siempre que éste se autentique (de acuerdo con la subsección 3.1 sobre autenticación), o lo solicite por teléfono comunicando el pin del certificado.

### 4.3 Solicitud de revocación cuando un usuario abandona la institución

La secretaría de recursos humanos del CIN2, ICMAB, CSIC o del ICN informa a la RA siempre que hay una baja de personal, ya sea local o visitante. La RA procede entonces a emitir la solicitud de revocación de certificado.

## Anexo I - Solicitud de certificado de usuario pkIRISGrid

### Solicitante

Nombre	
Apellidos	
Dirección email	
DN del certificado	/DC=es/DC=irisgrid/
Código de solicitud	
Fecha de emisión	
Dpto. / Proyecto	
Propósito de uso	
He leído y acepto las condiciones de pkIRISGrid y de la RA CSIC-Bellaterra descritas en los documentos: <a href="http://pki.irisgrid.es/policy/">http://pki.irisgrid.es/policy/</a> <a href="https://pki.irisgrid.es/rat38/policy/">https://pki.irisgrid.es/rat38/policy/</a>	
Fecha y firma	

### Jefe Departamento / Investigador Principal Proyecto

Nombre	
Apellidos	
Fecha sello y firma	

### Operador de la Autoridad de Registro (RA)

Nombre	
Apellidos	
Fecha y firma	

Nota: El solicitante debe asegurarse de cumplir los requisitos expuestos en los documentos correspondientes a las políticas de la RA CSIC-Bellaterra de pkIRISGrid y del propio pkIRISGrid. La aprobación de esta solicitud está sujeta a las normas descritas en este documento.

## Anexo II - Solicitud de certificado de servidor pkIRISGrid

Solicitante

Nombre	
Apellidos	
Dirección email	
DN del certificado	/DC=es/DC=irisgrid/
Código de solicitud	
Fecha de emisión	
Dpto. / Proyecto	
Propósito de uso	
He leído y acepto las condiciones de pkIRISGrid y de la RA CSIC-Bellaterra descritas en los documentos: <a href="http://pki.irisgrid.es/policy/">http://pki.irisgrid.es/policy/</a> <a href="https://pki.irisgrid.es/rat38/policy/">https://pki.irisgrid.es/rat38/policy/</a>	
Fecha y firma	

Administrador del servidor

Nombre	
Apellidos	
Dirección email	

Jefe Departamento / Investigador Principal Proyecto

Nombre	
Apellidos	
Fecha sello y firma	

Operador de la Autoridad de Registro (RA)

Nombre	
Apellidos	
Fecha y firma	

Nota: El solicitante debe asegurarse de cumplir los requisitos expuestos en los documentos correspondientes a las políticas de la RA CSIC-Bellaterra de pkIRISGrid y del propio pkIRISGrid. La aprobación de esta solicitud está sujeta a las normas descritas en este documento. Cuando solicite el certificado desde su navegador, en el apartado "Identificador IRISGrid", deberá introducirse 'host' como nombre del servicio.

## Anexo III - Revocación de certificado de usuario

Causa por la que se revoca el certificado

- A petición del usuario, comunicando el PIN del certificado.
- El usuario termina su vinculación laboral con el centro al que pertenecía y que le daba derecho a solicitar el certificado.
- El usuario utiliza su certificado para usos ajenos a la actividad que desarrolla la institución a la que pertenece, o bien de forma indebida.
- El usuario comparte su certificado o le da otros usos incompatibles con el objetivo de un certificado digital.
- Se ha detectado que el certificado es usado por varias personas.
- Se sospecha de un robo de la clave privada.
- Otras (especificar)

--

Solicitante

Nombre	
Apellidos	
Dirección email	
DN del certificado	/DC=es/DC=irisgrid
Código de solicitud	
Fecha de finalización	
Fecha y firma	

Jefe Departamento / Investigador Principal Proyecto

Nombre	
Apellidos	
Fecha sello y firma	

Operador de la Autoridad de Registro (RA)

Nombre	
Apellidos	
Fecha y firma	

## Anexo IV - Revocación de certificado de servidor

Causa por la que se revoca el certificado

- Deja de ofrecerse el servicio para el que se pidió el certificado de servidor.
- Se ha detectado que el certificado está instalado en varias máquinas, sin ser un sistema de alta disponibilidad.
- Se ha detectado que la clave privada del servidor se ha visto comprometida.
- Otras (especificar)

--

Solicitante

Nombre	
Apellidos	
Dirección email	
DN del certificado	/DC=es/DC=irisgrid
Código de solicitud	
Fecha de finalización	
Fecha y firma	

Administrador del servidor

Nombre	
Apellidos	
Dirección email	

Jefe Departamento / Investigador Principal Proyecto

Nombre	
Apellidos	
Fecha sello y firma	

Operador de la Autoridad de Registro (RA)

Nombre	
Apellidos	
Fecha y firma	