



Política de la Universidad de Cantabria como RA de pkIRISGrid

Versión: 1.0.3

Santander, 1 de Marzo 2010

Historia

Fecha	Versión	Cambio	Responsable
18/11/2009	1.0.0	Creación del Documento	Antonio S. Cofiño
23/11/2009	1.0.1	Revisión del Documento	Valvanuz Fernández
10/12/2009	1.0.2	Revisión del Documento	Antonio S. Cofiño
01/03/2010	1.0.3	Modificación de solicitantes a los que esta RA representa	Antonio S. Cofiño

Índice

1. Presentación.....	5
2. Operadores de la RA	5
3. Aprobación de solicitudes del certificado	5
3.1. Autenticación del solicitante	5
3.1.1. Reunión personal	5
3.2. Verificación del solicitante	6
3.2.1. Procedimiento de certificación de personas físicas	7
3.2.2. Procedimiento de certificación de servidor	7
3.2.3. Documentación archivada	7
4. Políticas de renovaciones.....	7
4.1. Solicitud de renovaciones 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

1. Presentación

En este documento se expone la política de la Universidad de Cantabria (UC) como Autoridad de Registro (RA) de infraestructura pkIRISGrid. La política que se describe se aplicará a las solicitudes de certificados recibidas después de la fecha de aceptación de este documento.

2. Operadores de la RA

Los operadores de la RA de UNICAN han de ser personal contratado o funcionario de la Universidad de Cantabria. Deben de haber sido formados para su cometido por personal de pkIRISGrid o por otros administradores de la RA de UNICAN.

En el momento en que un administrador deje su puesto, los restantes cambiarán la contraseña de administrador.

3. Aprobación de solicitudes del certificado

La RA de UNICAN aprueba solicitudes de certificado siempre y cuando se soliciten para los dominios de los centros, departamentos e institutos asociados a la Universidad de Cantabria y el solicitante sea miembro de la Universidad de Cantabria, o colabore como investigador.

3.1. Autenticación del solicitante

El proceso de autenticación del solicitante de un certificado será el mismo tanto para solicitudes de certificado de usuario como de servidor. La forma básica de autenticación del solicitante de certificado es la reunión cara a cara.

3.1.1. Reunión personal

La única forma actualmente de autenticar el solicitante de certificado es la reunión cara a cara. El solicitante deberá desplazarse a la RA de la Universidad de Cantabria ubicada en el departamento de Matemática Aplicada y Ciencias de la Computación en la Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. de las Castros, s/n 39005 Santander. El solicitante presentará su documento de identidad y comunicará su PIN al administrador. Éste generará la documentación necesaria que será archivada y determinará si

sigue adelante con el procedimiento de validación o no. Una vez aprobada, el administrador de la RA enviará la solicitud a la CA en el plazo de cinco días laborables.

3.1.1.1. Detalle de la reunión

La cita, indicando el día y la hora de la reunión, se acordará por correo electrónico con el administrador en cuestión.

3.1.1.2. Documentos aceptados

Los documentos aceptados son los siguientes:

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

En el proceso de autenticación del solicitante, el administrador de la RA contrastará los datos de la solicitud del certificado con los del documento de identidad presentado. Si los datos son correctos, se guardará toda la información, junto con los datos y la fecha del certificado para futuras auditorías.

3.1.1.4. Otros métodos

No aplicable.

3.2. Verificación del solicitante

Tras la autenticación del solicitante, se ha de verificar la autoridad de éste para solicitarlo antes de aprobar la solicitud. En todos los casos se verificará la dirección de correo electrónico.

3.2.1. Procedimiento de certificación de personas físicas

En la reunión cara a cara se comprobará a través de la base de datos de la Universidad de Cantabria que el solicitante puede solicitar un certificado.

3.2.2. Procedimiento de certificación de servidor

La persona solicitante deberá presentar un documento firmado por el responsable de los recursos que autoricen al solicitante a pedir un certificado de servidor, también se deberá indicar la persona que administra el servidor. Este documento se guardará junto con los documentos generados en la fase de autenticación.

3.2.2.1. Cambio de administrador para el servidor

En el supuesto 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 3.2.2, pero no será necesario volver a solicitar el certificado.

3.2.3. Documentación archivada

Descrito en el apartado 3.1.1.3

4. Políticas de renovaciones

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 renovaciones por iniciativa de la RA

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

- En el caso de un usuario:
 - Cuando el usuario utilice su certificado para usos ajenos a la actividad que desarrolla la institución a la que pertenece, o bien de forma indebida.
 - Cuando se detecta que el certificado es usado por varias personas.
 - Cuando se sospecha de un robo de la clave privada.
 - Cuando el usuario comparte su certificado o le da otros usos incompatibles con el objetivo de un certificado digital.
 - Cuando el usuario deja de tener permiso por 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 de la Universidad de Cantabria.
- 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 sección de recursos humanos de la Universidad de Cantabria 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.