# Política de la Universidad de Valladolid como oficina de registro (RA) de pkIRISGrid

## 1. Presentación

PkIRISGrid es la infraestructura de clave pública (PKI) usada en la iniciativa nacional de Grid IRISGrid.

PkIRISGrid fue acreditada el 25 de enero de 2006 por la EUGridPMA, organización internacional dedicada a la coordinación de la red de confianza entre las PKI que dan servicio a la e-Ciencia europea. De este modo se establecen los requisitos mínimos exigibles a los proveedores de identidad y se establece una red común de confianza aplicable a la autenticación de las entidades, servidores y usuarios finales para el acceso a los recursos distribuidos en el Grid.

La Universidad de Valladolid se incorpora a la red de oficinas de registro (RA) que colaboran con la autoridad de certificación (CA) de pkIRISGrid en la emisión de los certificados indispensables para el uso de IRISGrid.

En este documento se detalla la poítica de funcionamiento de la UVa como RA.

## 2. Operadores de la RA

La Subdirección de Redes del STIC se encarga de la formación y supervisión de los operadores de la RA. En un principio tendrán su sede en el Centro de Atención al Usuario de servicios TI; con domicilio en el Edificio Alfonso VIII, C/Real de Burgos S/N de Valladolid.

Sólo podrán nombrarse operadores de la RA a personas cuyo puesto de trabajo esté relacionado con las TI. Están destinados principalmente en el Servicio de Tecnologías de la Información y de las Comunicaciones, aunque existen operadores y técnicos destinados en otras unidades.

Se aplicarán los protocolos necesarios de seguridad en el uso de plataformas informáticas y de autentificación de los solicitantes. En particular se velará por la seguridad de las claves, cambiándose cada vez que algún operador deje de serlo.

Si fuera necesario preparar más sedes en otros campus dentro o fuera de Valladolid, se generará una nueva versión de estas políticas incluyendo estos detalles.

# 3. Aprobación de solicitudes de certificado

La función principal de una RA es comprobar que el solicitante es quien dice ser y que tiene autoridad para solicitar el certificado.

Será requisito previo para la emisión de certificados de usuario o de servidor la pertenencia a algún colectivo universitario relacionado con la investigación que pueda beneficiarse del acceso a IRISGrid, así como su compromiso de respetar sus normas de uso.

La autenticación del solicitante se realizará de una única forma, consistente en una reunión personal. Cuando se perciba que el número de solicitudes podría ser elevado, se estudiará una forma alternativa basada en correo electrónico firmado digitalmente; con la consecuente renovación de este documento de políticas de uso.

## 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*

Una vez que el usuario ha solicitado su certificado desde su navegador y haya sido contactado por un operador de RA, se desplazará al CAU referido en el punto 2 en la fecha y hora acordados en dicho contacto.

Presentará su DNI o pasaporte y comunicará su pin al operador.

El operador de la RA revisará y completará la documentación, resolverá la solicitud y la archivará.

En el caso de no aprobarse,informará al solicitante de la posibilidad de revisión directa por la Subdirección de Redes.

En el caso de aprobación, 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*

Se celebrará en el Centro de Atención al Usuario de servicios TI, CAU, referido en el punto 2. El horario es de 8 a 20 horas, y se concertará la cita adaptándose lo más posible a la disponibilidad del solicitante.

#### *3.1.1.2 Documentos Aceptados*

El operador de la RA contrastará los datos de la solicitud del certificado con los del documento de identidad presentado.

Los documentos aceptados son los siguientes, siempre en vigor e incorporando fotografía:

- Ciudadanos españoles: DNI.
- Ciudadanos comunitarios: Pasaporte o documento de identidad legal en su país de origen.
- Ciudadanos extranjeros: Pasaporte o NIE.

#### *3.1.1.3 Documentación archivada*

La RA archivará las fotocopias de los documentos de identidad y de la solicitud.

Todas las hojas fotocopiadas incorporarán la fecha y firma del solicitante.

### 3.2 Verificación del solicitante

El permiso para solicitar o usar un certificado de acceso a IRISGrid será concedido por el director de la unidad (centro o departamento) o por la dirección del STIC.

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

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

El CAU dispone de los medios necesarios para comprobar en línea la pertenencia del solicitante a un colectivo universitario y la relación exacta que tiene con la universidad.

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

El solicitante presentará un escrito que le autorice a presentar la solicitud del certificado firmado por el PER de la institución, por el administrador del sistema y por su responsable (centro, departamento, instituto, etc.)

#### *3.2.3 Documentación archivada*

La RA imprimirá y archivará los datos que acreditan la relación del solicitante con la Universidad. Para certificados de servidor, también se archivará la autorización conjunta del PER y del responsable del servidor.

# 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
- la circunstancias que provocaron la solicitud
- fecha
- anexos de otros otros documentos que pudieran justificar la revocación.

## 4.1 Solicitud de revocaciones por iniciativa de la RA

La RA solicitará la revocación de un certificado de usuario cuando

- Se están usando los servicios a los que tiene acceso para fines ajenos a la unidad que lo solicitó.
- 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 privada.
- El usuario comparte su certificado o le da otros usos ajenos a pkIRISGrid.
- El usuario deja de tener permiso de la unidad (centro, departamento, instituto, etc.) que le autorizó a usar el certificado.
- Otros usos del certificado objetivamente incorrectos o que puedan dañar la imagen o la reputación de pkIRISGrid o de la Universidad de Valladolid.

La RA solicitará la revocación de un certificado de servidor cuando

- 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

El CAU, además de tener acceso permanente a los datos del personal, repasa a diario el conjunto de bajas para la actualización de diversos procesos. En particular se cruzarán esos datos con el conjunto de certificados en vigor para solicitar las revocaciones que fueran necesarias.