Centro Extremeño de Tecnologías Avanzadas
CIEMAT

PKIRISGRID POLICY

Version 1.0

20-04-2009

Control de Cambios

Versión	Fecha	Comentario	Autor
0.1	30-03-2009	Creación del documento	Raúl Priego Martínez
1.0	20-04-2009	Mofication al nombrar pkIRISGrid	Raúl Priego Martínez

1. **Presentación.**
    1. Propósito.

Este documento define la política de la RA perteneciente a pkIRISGrid del Centro Extremeño de Tecnologías Avanzadas CIEMAT (a partir de ahora CETA-CIEMAT) . Con él se pretende establecer las bases necesarias para su correcta implantación.

2. Alcance.

Este documento se aplicará al personal del CETA-CIEMAT así como aquellos investigadores vinculados a esta institución que requieran certificados pkIRISGrid para acceder a los proyectos de e-Ciencia. Así mismo también cubrirá las necesidades de aquellas comunidades investigadoras próximas a CETA-CIEMAT cubriendo la ausencia de RA propias.

2. Operadores de la RA.

Los operadores de la RA CETA-CIEMAT deben ser trabajadores del CETA-CIEMAT y con conocimientos específicos de informática y especialmente de seguridad

Los operadores de la RA CETA-CIEMAT serán formados en sus labores por personal de pkIRISGrid u otros operadores de la RA. En caso de baja de un operador esta será comunicada a Rediris para la actualización de los datos de los operadores de la RA y los restantes operadores cambiaran la contraseña del mismo.

3. Aprobación de solicitudes de certificado.

La RA CETA-CIEMAT puede aprobar solicitudes de certificados tanto de usuarios como de servidores para sus miembros.

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 de autenticación del solicitante de certificado será cara a cara.

1. Reunión cara a cara

Una vez que el solicitante pide un certificado en la página web de la RA, un operador contactará con el vía correo electrónico para concertar una reunión. En dicha reunión el solicitante deberá autenticarse mediante un documento de identidad válido, y comunicará su pin al operador. Éste procederá a generar la documentación necesaria, archivarla y aprobar la solicitud.

Una vez aprobada, el operador de la RA enviará la solicitud a la CA de pkIRISGrid en el plazo de una semana.

2. Documentos aceptados

Los solicitantes deben presentar fotocopia y original de cualquiera de los documentos de identidad aceptados por la legislación española:

- DNI o pasaporte si el solicitante es ciudadano español.
- Pasaporte, si el solicitante es extranjero.

3. 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 guardará toda la información, junto con los datos y la fecha del certificado para futuras auditorías.

2. Verificación del solicitante

1. Procedimiento para personas físicas

El solicitante presentará en la reunión cara a cara un documento de pertenencia al CETA-CIEMAT o de pertenencia a un departamento de investigación vinculado al CETA-CIEMAT firmado por el responsable de dicho departamento que lo acredite como tal.

2. Procedimiento de certificación del servidor.

La persona solicitante deberá presentar un documento firmado por el responsable del recurso que autorice al solicitante a pedir un certificado de servidor. Este documento se guardará junto con los documentos generados en la fase de autenticación.

4. Política de revocaciones.

Esta sección describe 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 solicito, las circunstancias que provocaron la solicitud, la fecha, y otros documentos que justifiquen dicha decisión (como los datos de autenticación en caso de iniciativa del usuario, o informes que muestren el mal uso de los certificados).

1. Solicitud por revocación por iniciativa de la RA.

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

- En caso del un usuario:
  - Está usando los servicios a los que tiene acceso con su certificado de forma indebida.
  - Se detecta el robo de la clave privada
  - El usuario comparte su certificado o le da otros usos incompatibles con el objetivo del certificado digital.
  - El usuario deja de tener vinculación con el CETA-CIEMAT o con la institución bajo la cual se creo la certificación.
  - Otros usos del certificado que el operador estime incorrectos o que puedan dañar la reputación o la imagen de pkIRISGrid o del CETA-CIEMAT.
- En caso de certificados de 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.

2. Solicitud de revocaciones por iniciativa del usuario certificado.

   La RA solicitará la revocación de un certificado a petición del usuario siempre que éste se autentique (de acuerdo con la sección 3.1 sobre autenticación).

3. Solicitud de revocación cuando un usuario abandona la institución.

Los solicitantes deber informar a la RA cuando se produzca un cambio en su relación con el CETA-CIEMAT o con el grupo de investigación bajo cuyo amparo se solicitó el certificado.