Política para la RA de pkIRISGrid de la UPV/EHU

v: 1.0.0

Vitoria-Gasteiz, 2 de Julio de 2008

Universidad del País Vasco Euskal Herriko Unibertsitatea

Tabla de contenidos

Historia:

26/04/2008	Redacción y formato	Juan Carlos Varona
	Revisión	

1. Presentación

Este documento describe el conjunto de reglas y practicas operacionales que serán utilizadas por la Autoridad de Registro (RA) de la UPV/EHU para publicar solicitudes de certificados de pkiIRISGrid.

IRISGrid es la infraestructura para apoyar las actividades de la e-ciencia proporcionada por RedIRIS.

La UPV/EHU está afiliada a RedIRIS desde 1989, y en la actualidad trabajan en ella más de tres mil profesores, que participan activamente en proyectos de e-ciencia, así como investigadores internacionales, procedentes de programas de colaboración internacional con otros centros afines.

La activa participación, tanto de los investigadores locales como de los visitantes en la infraestructura de grid dependiente de pkiIRISGrid hace necesaria la creación de una RA de pkiIRISGrid en la UPV/EHU.

2. Operadores de la RA

Siguiendo las recomendaciones de pkiIRISGrid, los operadores de la RA de la UPV/EHU deben ser personal de la UPV/EHU con contrato estable, con más de dos años de experiencia en la UPV/EHU, y con conocimientos medios de informática.

Todos los operadores de la RA de la UPV/EHU deben haber sido formados para su labor por personal de pkIRISGrid u otros operadores de la RA de la UPV/EHU

Cuándo un operador deja de serlo o abandona la UPV/EHU, los restantes operadores cambian la contraseña de operador.

3. Aprobación de solicitudes de certificado.

La RA de la UPV/EHU aprueba solicitudes de certificado tanto de usuario como de servidor para sus investigadores.

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 forma básica de autenticación del solicitante de certificado es la reunión cara a cara.

Una vez que ha solicitado su certificado desde su navegador y haya sido contactado por un operador de RA, el solicitante se desplazará a la RA de la UPV/EHU, presentará un documento de identidad aceptado, y comunicará su pin al operador. Éste procederá a generar la documentación descrita más abajo, archivarla, y aprobará la solicitud.

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 de la UPV/EHU está situada en la sede del CIDIR de Alava (Edificio Las Nieves, C/Nieves Cano 33, 01006 Vitoria-Gasteiz). 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 Aceptados

Los ciudadanos podrán presentar cualquiera de los documentos de identidad aceptados por la legislación (DNI, o pasaporte). El carné de la UPV/EHU no se aceptará para autenticación, ya que no tiene fotografía.

Los ciudadanos comunitarios podrán presentar el pasaporte o un documento de identidad similar legal en su país de origen, siempre que este tenga fotografía.

Los ciudadanos no comunitarios deberán presentar su pasaporte.

3.1.1.3 Documentación archivada

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

3.1.2 Otros métodos

No aplicable.

3.2 Verificación del solicitante

Tras la autenticación del solicitante, se debe 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 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 su carné de la UPV/EHU.

El carné se fotocopiará y se guardará junto a las fotocopias de los documentos que se hicieron en la fase de autenticación.

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.

3.2.2 Descripción del procedimiento para certificado de servidor

En el caso de que se solicite un certificado de servidor, la fase de verificación de autoridad se hará en la reunión cara a cara seguidamente de la fase de autenticación.

La persona solicitante deberá presentar un documento firmado por el responsable de la máquina que autoricen al solicitante a pedir un certificado de servidor. Este documento o documentos se guardarán junto con los documentos generados en la fase de autenticación.

3.2.3 Documentación archivada

Descrito en los apartado 3.2.1 y 3.2.2.

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, 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.

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 a la UPV/EHU 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 privada.
  - 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 de la UPV/EHU

- 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

Cuando la Vicegerencia de Personal de la UPV/EHU informe a la RA de una baja de personal, ya sea local o visitante, esta procederá a emitir la solicitud de revocación de certificado.

5. Consideraciones especiales

En lo referente al ámbito de este documento, la UPV/EHU ha delegado en la Fundación Donostia International Physics Center (D.I.P.C.) la gestión de las solicitudes de certificado de servidor de pkiIRISGrid correspondientes al subdominio sw.ehu.es

Este subdominio es gestionado por la RA21 del D.I.P.C.