Ejemplo de política para una RA ficticia de pkIRISGrid

v: 1.0.0

Sevilla, 15 de Noviembre 2007

Índice de contenido

Política de la RA del Instituto de Investigación del Vino de Naranja (IIVN)

Política de ejemplo de una RA de un centro de investigación ficticio.

Historia:

07/11/2007	Salvador	Redacción.
14/11/2007	Salvador	Revisión y formato.
15/11/2007	Salvador	Cambiado el punto 3.2.1.2

1. Presentación

Se presenta en este documento la política de la RA del IIVN.

El IIVN, situado en Sevilla, es un instituto dedicado a la investigación de las propiedades del vino de naranja, a las técnicas de producción y a su promoción internacional.

El IIVN está afiliado a RedIris desde 1999, y en la actualidad trabajan en él más de 20 investigadores que participan activamente en proyectos de eCiencia haciendo uso de pkIRISGrid, así como más de 10 investigadores internacionales al año, 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 hacen necesaria la RA del IIVN, que lleva activa desde 2005.

2. Operadores de la RA

Los operadores de la RA del IIVN han de ser personal del IIVN con contrato estable, con más de dos años de experiencia en el IIVN, y con conocimientos medios de informática.

Todos los operadores de la RA del IIVN deben haber sido formados para su labor por personal de pkIRISGrid u otros operadores de la RA de IIVN.

Cuándo un operador deja de serlo o abandona el IIVN, los restantes operadores cambian la contraseña de operador.

3. Aprobación de solicitudes de certificado.

La RA del IIVN 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 del IIVN, 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 del IIVN está situada en la sede central del mismo instituto (C/ Matéos Gago 65, Sevilla). 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 españoles podrán presentar cualquiera de los documentos de identidad aceptados por la legislación española (DNI, o pasaporte). El carné del IIVN 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 los de el documento de identidad presentado. Si los datos son correctos, se fotocopiará el documento, y se guardará, junto con los datos y la fecha del certificado para futuras auditorías.

3.1.2. Certificado digital

Los ciudadanos españoles podrán autenticarse mediante el envio de un correo electrónico firmado con un certificado a su nombre emitido por una autoridad de certificación reconocida por la legislación española (CNMT, Policía Nacional). Independientemente de la nacionalidad, también se admite un correo electrónico firmado por un certificado válido de pkIRISGrid a nombre del solicitante.

Esta opción está disponible sólo para certificados personales, no de servidor.

3.1.2.1 Detalle de la solicitud

En el correo electrónico deberá incluir el nombre del solicitante y, adjunta, una captura de pantalla del navegador en la última etapa de solicitud del certificado (en la que salen los datos del certificado).

Los datos de la captura de pantalla se cotejarán con la solicitud, y el propio correo electrónico se exportará a texto plano, y se comprobará la firma con OpenSSL versión 0.9.8e 23 Feb 2007.

3.1.2.2 Certificados aceptados

Se admiritán para esta modalidad de autenticación certificados personales emitidos por una autoridad de certificación reconocida por la legislación española (CNMT, Policía Nacional), así como certificados personales válidos de pkIRISGrid.

3.1.2.3 Documentación

Se guardará el correo electrónico firmado exportado en texto plano en formato digital para auditoría, en los servidores del IIVN.

3.1.3 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 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 del IIVN. 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.

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

3.2.1.2 Verificación de una solicitud con certificado digital

En caso de que la solicitud de certificado se haya realizado mediante el envío de un correo electrónico firmado, el solicitante enviará además los documentos necesarios para la verificación descritos en el apartado anterior, escaneados y adjuntos en el correoelectrónico.

Se generará un informe que describa la situación del solicitante en la empresa en la fecha de la solicitud, con la fecha de la comprobación y el nombre del operador de la RA, y se guardará en formato digital, junto al propio correo electrónico enviado por el solicitante y sus archivos adjuntos.

3.2.2 Descripción del procedimiento para certificado de servidor

En el caso de que se solicite un certificado de servidor, la posibilidad de autenticaciónmediante correo electrónico firmado no estará disponible, por lo que 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 PER del IIVN y 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 generadosen 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, 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 IIVN 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 IIVN.
- 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 queéste 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 IIVN informa a la RA siempre que hayuna baja de personal, ya sea local o visitante. La RA procede entonces a emitir la solicitud de revocación de certificado.