Universidad de Alcalá

SERVICIOS INFORMÁTICOS

Servicio de Explotación y Seguridad Informática

Política de la Autoridad de Registro UAH de pkIRISGrid

Versión 1.0.0

Alcalá de Henares, 24 de septiembre de 2008

Índice de contenido

1. Revisiones del documento

Versión	Fecha	Autor	Actividad
	23/09/2008	Ángel Javier Álvarez Miguel	Propuesta de borrador
1.0.0	24/09/2008	José Francisco Ríos Balsalobre	Redacción del documento

2. Presentación

Se presenta en este documento la política y los procedimientos operativos de la Autoridad de Registro Universidad de Alcalá (en adelante UAH) para pkIRISGrid.

La Autoridad de Certificación pkIRISGrid no realiza el rol de Autoridad de Registro. Por tanto, la creación de esta RA UAH de pkIRISGrid tiene como objetivo asumir el rol de Autoridad de Registro para los miembros y servidores de la UAH que quieran participar en IRISGrid.

IRISGrid es la infraestructura para soportar las actividades de e-ciencia proporcionadas por la Red Nacional de Investigación y Educación RedIRIS.

La UAH es una institución moderna, de tamaño medio, reconocida en Europa y América como modelo a imitar. A los clásicos estudios humanistas y de ciencias sociales, la UAH ha incorporado las más novedosas titulaciones en todos los campos científicos como las ciencias de la salud o distintas ingenierías distribuidas en sus diversos campus, que constituyen todas ellas, junto con el Parque Científico y Tecnológico, un factor decisivo de proyección internacional y de elemento dinamizador de la actividad en nuestra región.

Sus casi 25.000 alumnos, 1.700 profesores y 800 trabajadores administrativos y de servicio dan vida a 41 Titulaciones Oficiales, 15 Programas Oficiales de Postgrado, 43 Doctorados (15 de ellos con Mención de Calidad) y una importante oferta de Másteres y Estudios de Especialización. La reconocida calidad de sus estudios, el desarrollo de importantes líneas de investigación, sus relaciones internacionales, el interés histórico-artístico de sus emblemáticos edificios, sus nuevas y modernas instalaciones y su completa adaptación a las demandas del actual mercado de trabajo la sitúan a la vanguardia de las universidades públicas.

Los Servicios Informáticos de la UAH son la unidad organizativa responsable de los sistemas de información y de comunicaciones utilizados para el apoyo, en óptimas condiciones de calidad, coste y plazo, a las actividades de docencia, investigación y gestión operativa y estratégica de la UAH.

3. Operadores de la RA

Los operadores de la RA UAH han de ser personal funcionario perteneciente a la relación de puestos de trabajo de los Servicios Informáticos, con puesto de trabajo operador de sistemas o superior y más de 6 meses de antigüedad en el puesto.

Todas las designaciones y exclusiones de operadores de la RA UAH serán realizadas por el Director de los Servicios Informáticos o, en su ausencia, por el Jefe de Explotación y Seguridad Informática, e informadas a RedIRIS por el procedimiento que defina al efecto.

La password de operador para realizar las operaciones de la RA UAH será compartida por los operadores y conocida en todo momento por el Director de los Servicios Informáticos y el Jefe de Explotación y Seguridad Informática. Cualquier exclusión de operadores requiere un cambio de password inmediato. En todo caso la password se cambiará en un plazo máximo de 6 meses desde el último cambio.

Los operadores serán informados y conocerán con antelación a las operaciones el manual de operador de una RA de pkIRISGrid.

4. Aprobación de solicitudes de certificado.

La RA UAH de pkIRISGrid, desempeñada por los Servicios Informáticos de la UAH, será la encargada de aprobar las solicitudes de certificados, tanto de usuario como de servidor, del personal de la UAH interesado en participar en la infraestructura IRISGrid.

Sólo se aceptarán solicitudes de interesados en la tecnología GRID, su desarrollo, implantación y aplicaciones y que pertenezcan a los siguientes colectivos:

- Personal docente e investigador (PDI) de la UAH con proyectos o intereses en la tecnología GRID.
- Personal de administración y servicios (PAS) de la UAH que realicen actividades de apoyo y colaboración con grupos de investigación o proyectos relacionados con la tecnología GRID.
- Alumnos de la UAH que realicen trabajos o proyectos relacionados con la tecnología GRID, con el aval necesario del Jefe del Departamento donde esté realizando dichas actividades.

4.1 Autenticación del solicitante

El solicitante deberá autenticarse, después de su solicitud, ante el responsable de la RA UAH.

La forma única de autenticación del solicitante es mediante identificación presencial por parte de un operador de la RA UAH.

4.1.1 Identificación presencial

Una vez solicitado el certificado desde su navegador y haya sido contactado por un operador de la RA UAH, el solicitante se desplazará a la RA UAH en el horario y fecha acordado con el operador, presentará un documento de identidad aceptado y comunicará su PIN al operador. Éste procederá a revisar el documento, generar la documentación descrita más adelante, su archivo y determinará e informará al solicitante si se acepta o rechaza la solicitud.

Una vez aprobada, el operador de la RA enviará la solicitud a la CA en el plazo de dos días laborables.

4.1.1.1 Detalles de la reunión cara a cara

La RA UAH está situada en el edificio de Servicios Informáticos de la UAH en el Campus externo de Alcalá de Henares. El acceso al Campus se realiza desde la N-

II en sentido Guadalajara por la ctra. de Meco, s/n y en sentido Madrid en el km. 33,600.

El horario de atención al cliente es de 9 a 14 y de 16 a 18 de lunes a jueves y de 9 a 14 los viernes, si bien el solicitante deberá previamente acordar la reunión con el operador y ésta deberá tener lugar en el plazo máximo de 7 días hábiles.

Al llegar al edificio de Servicios Informáticos el solicitante deberá dirigirse a la Sección de Sistemas y preguntar por el operador con el que acordó la reunión.

4.1.1.2 Documentos aceptados para la autenticación

El solicitante deberá llevar consigo un documento de identificación y una fotocopia del mismo, de la cara en la que se encuentre la fotografía, que entregará al operador para su archivo. Los documentos aceptados son los siguientes:

- Los ciudadanos españoles podrán presentar cualquiera de los documentos de identidad aceptados por la legislación española (DNI, DNI electrónico o pasaporte).
- Los ciudadanos comunitarios podrán presentar el pasaporte o bien el documento de identidad propio de su país, siempre y cuando incluya fotografía.
- Los ciudadanos no comunitarios deberán presentar su pasaporte.

No se admitirán otros documentos para el propósito de la autenticación.

4.1.1.3 Documentación aportada para archivar

El operador contrastará los datos de la solicitud del certificado y la identidad del solicitante para determinar si se acepta la solicitud. Si es aceptada, recopilará y archivará los siguientes documentos:

- Copia de la solicitud aportada por el solicitante, donde marcará la fecha y hora de su presentación.
- Copia del documento de identificación aportada por el solicitante.
- En el caso de alumnos, el original de la autorización del Jefe de Departamento.

4.2 Verificación del solicitante

Una vez realizada la autenticación del solicitante en la reunión cara a cara se procederá a validar la solicitud consistente en comprobar que el solicitante pertenece a los colectivos autorizados y descritos al inicio del apartado 4.

4.2.1 Descripción del procedimiento para certificado de personas físicas

Utilizando el documento de identificación proporcionado por el solicitante se procederá a comprobar que dispone de una cuenta de usuario válida y vigente en el directorio de la UAH y el colectivo al que pertenece.

Si es un alumno se comprobará que es correcto el Director de Departamento que autoriza su solicitud.

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.

4.2.2 Descripción del procedimiento para certificado de servidor

El servidor debe estar en el inventario de la UAH y el solicitante debe aportar la siguiente información referente al mismo:

- Nº de inventario.
- MAC address.
- Nombre DNS (del dominio uah.es).
- Dirección IP.

El solicitante deberá presentar un documento firmado por el responsable del servidor, o por el Jefe del Departamento en su defecto, que autoricen al solicitante a solicitar un certificado de servidor. Estos 2 documentos se archivarán junto con los generados en la fase de autenticación.

5. Política de revocaciones

En esta sección se describen los supuestos en que la RA UAH solicitará 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.

5.1 Solicitud de revocaciones por iniciativa de la RA UAH

La RA solicitará la revocación de un certificado por iniciativa propia cuando ocurra uno o varios de los siguientes supuestos.

5.1.1 Revocación de certificados de usuario

En estos supuestos, el operador de la RA UAH revocará un certificado de usuario:

a. El usuario que solicitó el certificado deja de pertenecer al colectivo al que pertenecía cuando solicitó el certificado.
b. El usuario utiliza su certificado para fines distintos a las actividades autorizadas en el marco de esta política.
c. Se ha hecho un uso ilegítimo de las infraestructuras a las que se tiene acceso por el hecho de disponer de este certificado o que dañan la imagen o la reputación de IRISGrid, de la UAH o de otras entidades adheridas.
d. El usuario comparte su certificado con terceras personas.
e. Se sospecha de un robo de la clave privada o compromiso de la seguridad en el equipo donde reside el certificado.

5.1.2 Revocación de certificados de servidor

En estos supuestos, el operador de la RA UAH revocará un certificado de servidor:

a. Se sospecha de un robo de la clave privada o compromiso de la seguridad en el equipo donde reside el certificado.
b. Se da de baja el servidor.
c. Se reutiliza el servidor para otras actividades no relacionadas con IRISGrid.
d. Se ha hecho un uso ilegítimo de las infraestructuras a las que se tiene acceso por el hecho de disponer de este certificado o se daña la imagen o la reputación de IRISGrid, de la UAH o de otras entidades adheridas.

e. Se detecta que el certificado está instalado en 2 ó más equipos sin corresponder a una arquitectura de alta disponibilidad.
f. El usuario utiliza su certificado para fines distintos a las actividades autorizadas en el marco de esta política.

5.2 Solicitud de revocaciones por iniciativa del usuario del Certificado

La RA solicitará la revocación de un certificado de usuario cuando éste lo solicite y se autentique de acuerdo al procedimiento definido en la subsección 4.1.

Se archivará un documento junto a la documentación de la solicitud indicando el motivo de la revocación y la fecha y hora de la revocación.

5.3 Solicitud de revocación cuando un usuario deja la UAH

Cuando un usuario deja de pertenecer a la UAH deberá informar a la RA UAH del hecho y ésta revocará el certificado de usuario.

Se archivará un documento junto a la documentación de la solicitud indicando el motivo de la revocación y la fecha y hora de la revocación.