

Política de i2basque como autoridad de registro (RA) de pkIRISGrid

v: 1.0.0

Donostia-San Sebastián, 13 de Noviembre de 2009

Tabla de contenidos

1. PRESENTACIÓN.....	1
2. OPERADORES DE LA RA.....	1
3. APROBACIÓN DE SOLICITUDES DE CERTIFICADO.	1
4. POLÍTICA DE REVOCACIONES.....	3

Historia:		
13/11/2009	Redacción y formato – rev 1.0.0	Charo Sánchez Ojeda
03/06/2010	Autorización para la delegación de los dominios cicbiogune.es y cicbiogune.com –rev 1.1.0	Charo Sánchez Ojeda

1. Presentación

En este documento se describen el conjunto de reglas y los procedimientos operativos que serán utilizados por la Autoridad de Registro (RA) de I2BASQUE para publicar solicitudes de certificados de pkIRISGrid.

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

La política descrita en este documento se aplicará a las solicitudes de certificado recibidas después de la fecha de publicación de este documento.

2. Operadores de la RA

Siguiendo las recomendaciones de pkIRISGrid, los operadores de la RA de I2BASQUE deben ser personal de I2BASQUE, con más de dos años de experiencia en I2BASQUE, y con conocimientos medios de informática.

Todos los operadores de la RA de I2BASQUE deben haber sido formados para su labor por personal de pkIRISGrid u otros operadores de la RA de I2BASQUE.

Las designaciones y exclusiones de los operadores de la RA de I2BASQUE serán realizadas por el coordinador de la Red Académica I2BASQUE, e informadas a RedIRIS por el procedimiento que defina al efecto.

Cuando un operador deja de serlo o abandona I2BASQUE, los restantes operadores cambian la contraseña de operador.

3. Aprobación de solicitudes de certificado

El usuario podrá solicitar desde su navegador, en el enlace para la RA de I2BASQUE (<https://pk.irisgrid.es/rat24/>), su certificado de usuario o certificados de servidor.

La RA de I2BASQUE aprueba solicitudes de certificado tanto de usuario como de servidor para sus investigadores, para el dominio **i2basque.es**

Asimismo también aprobaremos solicitudes de certificados para los siguientes dominios correspondientes a entidades afiliadas que han delegado en nuestra RA la gestión de su espacio de nombres:

<u>Dominio</u>	<u>Entidad Afiliada</u>
cicbiogune.es	CIC Biogune
cicbiogune.com	CIC Biogune

3.1. Autenticación del solicitante

La autenticación del solicitante será obligatoria, tanto en solicitudes de usuario como de servidor, y en ambos casos el proceso de autenticación del solicitante de certificados será el mismo.

Se seguirá el procedimiento detallado a continuación:

3.1.1. Reunión cara a cara

La única forma de autenticación del solicitante de certificado es mediante la reunión personal entre un operador de la RA y el solicitante.

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 I2BASQUE, 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 reunión será acordada mediante correo electrónico con un operador de la RA y se celebrará en la sede de I2BASQUE en la siguiente dirección:

- Parque Tecnológico de Miramón, en Paseo Mikeletegi, 69 – Torre Arbide Norte, 2009 San Sebastián

3.1.1.2 Documentos Aceptados

Los ciudadanos podrán presentar cualquiera de los documentos de identidad aceptados por la legislación (DNI, o pasaporte).

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 auditorías.

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 documento de identidad especificado en punto 3.1.1.2

El documento 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 apartados 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 I2BASQUE 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 I2BASQUE.
- 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 se informe a la RA de una baja de personal, ya sea local o visitante, esta procederá a emitir la solicitud de revocación de certificado.