

pkIRISGrid

Plantilla para la redacción de políticas de RA

v: 0.9.0

Sevilla, 2 de Marzo 2009

Índice de contenido

Índice de contenido.....	2
Resumen	3
Historia.....	3
Plantilla para la redacción de la política.....	4
1. Presentación.....	4
2. Operadores de la RA.....	4
3. Aprobación de solicitudes de certificado.....	4
3.1. Autenticación del solicitante.....	4
3.1.1. Reunión cara a cara.....	4
3.1.1.1 Detalles de la reunión.....	5
3.1.1.2 Documentos Aceptados.....	5
3.1.1.3 Documentación archivada.....	5
3.1.2. Otros métodos.....	5
3.2 Verificación del solicitante.....	5
3.2.1 Descripción del procedimiento para certificado de personas físicas.....	6
3.2.2 Descripción del procedimiento para certificado de servidor.....	6
3.2.2 Documentación archivada.....	6
4. Política de revocaciones.....	6
4.1 Solicitud de revocaciones por iniciativa de la RA.....	6
4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado.....	7
4.3 Solicitud de revocación cuando un usuario abandona la institución.....	7

Resumen

Este documento contiene una plantilla para la redacción de políticas de RA de pkIRISGrid. Está realizado para facilitar la labor de redactar una política a los responsables de RAs.

Intenta ser todo lo autocontenido posible, ofreciendo una descripción sobre qué hay que escribir en cada uno de los puntos, además de incorporar anotaciones para ayudar a comprender las responsabilidades y el funcionamiento de una RA.

Historia

02/03/2009	0.9.0	Javi Masa	Incorporación del carné de conducir, NIE y documentos de identidad válidos en países comunitarios como documentos acreditativos de identidad
27/02/2009	0.8.1	Javi Masa	Aclaración sobre el DNI (tanto electrónico como tradicional) y la no validez del uso del certificado almacenado en el DNI electrónico como método de autenticación
23/02/2009	0.8.0	Javi Masa	Eliminación de referencias relacionadas con el uso del DNI electrónico para la autenticación del solicitante
22/12/2008	0.7.0	Javi Masa	Modificaciones relacionadas con la autenticación del solicitante y el DNI electrónico
16/11/2007	0.6.0	Salvador Romero	Creación a partir del documento para la redacción de políticas de RA para pkIRISGrid.

Plantilla para la redacción de la política

1. Presentación

Esta sección se usa para la presentación del documento de la RA. Su contenido es abierto, y no hay datos concretos que haya que especificar. Puede ser usado para miscelánea.

2. Operadores de la RA

En esta sección se debe especificar quién puede ser operador de la RA, es decir, se han de enumerar las condiciones que debe cumplir una persona para ser nombrada operador de la RA.

No debe confundirse con quiénes son los operadores actuales de la RA por lo que no deben incluirse nombres de persona. Para ello se usará el documento de condiciones de uso de una RA o el documento de modificación de datos de operadores y dominios de la RA.

Sólo los operadores de la RA pueden administrarla, y deben conocer tanto la política de pkIRISGrid como la de su propia RA. Los nuevos operadores deben ser dados de alta notificándolo a los responsables de pkIRISGrid. Cuando se marcha un operador, se ha de cambiar la clave del administrador de la RA.

3. Aprobación de solicitudes de certificado

En esta sección se deberán detallar los pormenores de los trámites burocráticos que hay que realizar antes de aprobar una solicitud de certificado.

*Es misión de la RA dar fe de que la persona que solicita un certificado es quién dice ser, y que efectivamente tiene autoridad para solicitarlo. La política de la RA deberá **detallar** cómo la RA verifica la identidad de la persona (y la veracidad de todos los datos de la solicitud, como el teléfono y el correo electrónico) y que está autorizada para obtener un certificado.*

3.1. Autenticación del solicitante

La RA es responsable de verificar la identidad del solicitante. En esta subsección y sus diferentes apartados se deberán especificar los métodos por los que un solicitante puede autenticarse frente a la RA.

*Las RAs de pkIRISGrid deben comprobar la identidad del solicitante mediante una **reunión cara a cara**. No se permitirá otro tipo de autenticación. No será válido el envío de correo electrónico firmado con el certificado incluido en el DNI electrónico.*

Se debe especificar el proceso de autenticación en la política de la RA de forma detallada, y se recomienda que se publique una guía para sus usuarios.

3.1.1. Reunión cara a cara

Se describirá el proceso de reunión cara a cara entre el solicitante y el operador de RA. Este es el método obligatorio para todas las RA.

En la reunión cara a cara, el solicitante se desplaza a la RA y presenta un documento oficial

válido (DNI tradicional, DNI electrónico o pasaporte). Para los ciudadanos no españoles será necesario el pasaporte.

3.1.1.1 Detalles de la reunión

Aquí se detallarán los aspectos de la reunión no contemplados en los siguientes puntos, así como los requisitos particulares de cada RA.

La reunión cara a cara puede requerir una cita previa o no, según lo especificado en la política de RA.

3.1.1.2 Documentos Aceptados

Listado de documentos aceptados por la RA para la autenticación del solicitante. Los documentos aceptados son:

- Ciudadano español: **DNI** (tradicional, electrónico), **pasaporte** o permiso de **conducir**
- Ciudadano comunitario: **Pasaporte** o documento de **identidad legal propio de su país** de origen, siempre y cuando tenga fotografía
- Ciudadano no comunitario: **Pasaporte** o **NIE** (carné de Número de Identificación de Extranjeros). No se aceptarán NIE en tramitación, sólo definitivos con la tarjeta que muestre la fotografía

La RA deberá enumerar en su política los documentos oficiales aceptados de entre la lista de documentos permitidos.

En el caso de uso del DNI electrónico deberá mostrarse en la reunión cara a cara al operador de la RA. No será válido el envío de un correo electrónico firmado con el certificado incluido en el DNI electrónico para evitar la reunión cara a cara.

No será aceptable la tarjeta universitaria o similar, aunque tenga fotografía.

3.1.1.3 Documentación archivada

En este punto se detallarán el formato de la documentación generada en el proceso de la reunión cara a cara que se guardará para futuras auditorías.

La RA debe conservar una copia de el documento presentado, con fecha del día en que se presenta y con la firma del solicitante, en formato auditable, por ejemplo como una fotocopia del documento firmada por el solicitante. Igualmente el formato de esta copia debe estar especificado en la política de la RA.

3.1.2. Otros métodos

No se permiten, por el momento, otros métodos de autenticación. Si algún día se admiten otros métodos de autenticación para solicitantes de certificados, se deberán especificar con detalle en este punto.

3.2 Verificación del solicitante

Una vez que el solicitante de un certificado se ha autenticado, el siguiente paso es verificar que esta persona tiene permisos para solicitar y usar un certificado pkIRISGrid. Esta operación es un

trámite burocrático cuya complejidad o simplicidad depende mucho de la política de la RA en particular, y se detallará en esta subsección y los siguientes apartados.

El mecanismo escogido para la verificación de autoridad por la RA debe detallarse en la política de la RA, y una vez más se recomienda que se publique una guía para usuarios.

3.2.1 Descripción del procedimiento para certificado de personas físicas

En este apartado se detallarán los documentos exigidos al solicitante para verificar que puede solicitar un certificado, o se detallará el método utilizado para comprobarlo.

Esto lo puede demostrar el solicitante presentando algún documento u autorización.

Se debe guardar una copia de los documentos presentados en formato auditable, de forma similar a los documentos presentados en la autenticación.

3.2.2 Descripción del procedimiento para certificado de servidor

Similar al punto anterior, además hay que verificar que el solicitante está autorizado, por una persona competente, para administrar el servidor. Los pormenores de esta verificación se detallarán en esta sección.

En el caso de que el certificado se solicite para un servicio/servidor, el solicitante debe, además de autenticarse mediante reunión cara a cara, demostrar que tiene el permiso de su institución para solicita dicho certificado de servidor. De forma habitual, esta autorización vendrá dada por el responsable de la máquina para la que se solicita el certificado o por el administrador del dominio. El formato de la autorización debe estar especificado en la política de la RA, y esta debe ser almacenada en formato auditable.

3.2.2 Documentación archivada

En este apartado se detallará el formato de la documentación generada en la verificación del solicitante tanto para certificados de personas físicas como para certificados de servidor, que se guardará para futuras auditorías.

4. Política de revocaciones

En esta sección se deben cubrir las distintas circunstancias por las que una RA puede o debe solicitar la revocación de un certificado.

Básicamente existen tres circunstancias en las que una RA debe solicitar la revocación de un certificado: Mal uso del mismo, solicitud del usuario, y abandono de la institución por parte del usuario.

4.1 Solicitud de revocaciones por iniciativa de la RA

En esta subsección se deben describir los casos en los que la RA considera que se debe revocar un certificado, así como el formato de la documentación generada.

Los operadores de la RA pueden solicitar revocaciones de certificados siempre que tengan dudas razonables de que su clave privada ha sido comprometida, o de que se está haciendo un mal uso del mismo. La RA deberá solicitar revocaciones de certificados cuando entienda que se está

haciendo un mal uso de él o sospeche que la clave privada de un certificado se ha visto comprometida. Con cada solicitud de revocación se redactará un informe en el que se detallen los participantes, el certificado a revocar y el motivo, y se almacenará de forma auditable. Tanto el formato como la forma de almacenamiento deben estar detallados en la política de la RA.

4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado

En esta subsección se detallarán cómo puede un usuario solicitar la revocación de su certificado a través de su RA, y debe cubrir aspectos tales como la autenticación del usuario, documentación a presentar, el formato de la documentación que se genera para cubrir esta incidencia, etc.

Los usuarios pueden revocar sus certificados sin intervención de la RA, pero es posible que un usuario solicite a una RA que pida su revocación por él, en caso de que no recuerde los datos de revocación del certificado. En este caso la RA deberá también solicitar la revocación del certificado a petición del usuario, si bien el usuario deberá identificarse de forma similar a cuando efectuó la solicitud del mismo. En caso de que por diversos motivos el usuario no pueda identificarse de la forma descrita, el responsable de la RA siempre podrá revocar el certificado, siempre que esté razonablemente seguro de la identidad del solicitante o surjan dudas razonables de mal uso del mismo.

4.3 Solicitud de revocación cuando un usuario abandona la institución

En esta sección se describe como la RA detecta que un usuario abandona la institución a la que está asociado su certificado (circunstancia por la cual debe solicitar la revocación de éste). También se debe especificar la información que se genera para cubrir esta incidencia, y el formato en el que se guarda para auditoría.