Guía rápida del operador de una RA de pkIRISGrid

v: 0.3.0

Sevilla, 15 de Noviembre 2007

Guía rápida rápida del operador de una RA

Operadores

1. La RA debe ser administrada sólo por el operador u operadores designados, que deberán conocer proceder de acuerdo con la política de la CA y de su RA particular.
2. Se debe informar a los administradores de pkIRISGrid de la identidad de los operadoresde la RA siempre que haya un cambio.
    1. Los datos que se deben enviar son:
    2. Nombre y Apellidos.
    3. Dirección postal de la organización.
    4. Dirección de correo electrónico (a porder ser de la organización).
    5. Teléfono.

Solicitudes

1. Antes de aprobar una solicitud, el solicitante debe demostrarle a los operadores de la RA que, efectivamente, solicitó el certificado. Esto puede hacerse mediante:
    1. **Reunión cara a cara**: El solicitante debe desplazarse a la RA **en persona**, y pedir que se le apruebe la solicitud de certificado.
        1. El solicitante debe presentar en dicha reunión un documento oficial con foto que demuestre que es quien dice ser. La RA puede también admitir otros documentos (tarjeta de la institución o similares), siempre con fotografía. dependiendo de su política. Estos documentos deben estas especificados en la política de la RA, y no se admitirán otros.
        2. Así mismo el solicitante debe demostrar que pertenece a la institución desde la que solicita el certificado, y que tiene de dicha institución el permiso para obtenerlo . *
        3. Se guardará, para auditoría, una fotocopia de los documentos presentados del solicitante, fechada, y con firma del solicitante.
        4. La posibilidad de autenticación y validación de la solicitud mediante reunión cara a cara debe estar disponible en todas las RA.
    2. **Correo electrónico firmado digitalmente**: Si el solicitante poseyera un certificado de persona física reconocido por la legislación española (usuario de la FNMT-RCM clase 2 (persona física)), o un certificado válido de pkIRISGrid, podrá solicitar la aprobación de su solicitud de certificado enviando un correo electrónico firmado por su certificado a la RA, detallando el pin de la solicitud del certificado.
        1. Se guardará una copia digital e impresa de este correro electrónico, (incluyendo la firma digital), a efectos de auditoría.
        2. Una vez comprobada la identidad del solicitante, la RA debe comprobar la pertenencia del solicitante a la institución y su autoridad para solicitar el certificado, antes de aprobar la solicitud.
        3. La posibilidad de autenticación y validación de la solicitud mediante correo electrónico firmado digitalmente es optativo para cada RA. Deberá detallarse en la política de la RA si se ofrece o no, así como cuales de los certificados descritos anteriormente en el punto 2 se aceptan.

2. En el caso de que el certificado se solicite para un servidor, la persona responsable que lo solicita debe acreditarse de una forma segura (de la misma forma que en el apartado anterior). Además, debe demostrar que está autorizado para solicitar un certificado de servidor por el administrador del dominio o por el responsable de la máquina.
    1. El proceso de autenticar al solicitante y de comprobar su autorización debe estar detallado en la política de la PKI.
3. En cualquier caso, se deben solicitar certificados desde un navegador soportado por la PKI, instalado en un ordenador en el que sólo el solicitante tenga acceso a su certificado y a su clave privada.
    1. Los administradores de la RA deberán aconsejar a los usuarios para realizar la solicitud de acuerdo a la política.
    2. No se deberá animar en ningún caso a los solicitantes a solicitar un certificado desde un ordenador público o no controlado por el solicitante.
    3. No se aprobarán las solicitudes de certificado que se hayan sido solicitadas desde un ordenador no controlado por el solicitante.
4. Nunca se aprobaran solicitudes que hayan sido solicitadas por una tercera persona en nombre del solicitante.

Revocaciones

1. Los operadore de RA deberán revocar certificados por iniciativa propia cuando:
    1. Tengan dudas razonables de que la clave del certificado ha sido comprometida, o se tiene razones para sospechar que se está haciendo un mal uso del certificado.
    2. El dueño del certificado abandona la institución a la que está asociado su certificado.
2. Los operadores de la RA deben solicitar la revocación de certificados con la mayor prontitud posible desde que deciden que es necesaria

Comentarios:
* En muchos casos, todos los miembros de una institución tienen permiso para obtener un certificado de pkIRISGrid, con lo cual basta demostrar la pertenencia de la institución. En este caso, el punto dos y tres son muy similares.