Exportar el certificado con formato PKCS#12

Estas instrucciones describen como exportar su certificado desde su navegador web. Esto es necesario por dos razones:

En primer lugar para tener una copia de su certificado y de su copia privada por si le ocurre algo a la copia almacenada en su navedor (por si cambia de versión de navegador y su nueva versión no preserva la clave, por si tiene problemas con el ordenador, etc).

En segundo lugar es necesario exportar su certificado y clave privada para poder acceder al interface de trabajo con IRISGrid. Las instrucciones siguientes le indicarán cómo extraer el certificado y la clave como un conjunto en formato PKCS#12, que suele guardarse en un fichero con extensión .p12. Navegadores basados en Mozilla

Lo primero que debe hacer es acceder al gestor de certificados. A continuación se detalla cómo acceder a dicho gestor desde diferentes navegadores

Mozilla

> Ir a Preferences (Menú Edit en Linux/Windows?, Menú Mozilla en MAC OS) Bajo "Privacy & Security" ir a "Certificates" Seleccionar "Manage Certificates...

Firefox

> Ir a Preferences (Menú Edit en Linux/Windows?, Menú Firefox en MAC OS) Bajo "Advanced" ir a "Certificates" Seleccionar "Manage Certificates...

Galeon

> Ir a Edit > Preferences Ir a "Privacy" Seleccionar "Manage Certificates...

Una vez que se ha abierto el administrador de certificados (Certificate Manager):

> Elija su certificado y pulse sobre "Backup" Introduzca un nombre para el fichero, por ejemplo irisgrid-cert-backup.p12 Introduzca la clave para acceder al servicio de seguridad de su navegador (el sitio donde su navegador guarda internamente las claves) Introduzca una clave para protejer el fichero de backup

El fichero de backup (por ejemplo irisgrid-cert-backup.p12) será creado. Internet Explorer

> Ir a Tools - Internet Options - Content - Certificates - Personal (Card) Seleccionar el certificado de IRISGrid Seleccionar export Seleccionar la opción: include private key Selecciona: use stronger security Deseleccionar la opción: delete private key after export Introducir una clave para proteger las credendciales exportadas Elegir un nombre para el fichero, por ejemplo irisgrid-cert-backup

Esto creará un fichero con extensión .pfx que contiene su certificado y clave privada protegidas por la clave que ha proporcionado Notas generales

La clave de acceso al sistema de seguridad de su navegador es totalmente local a su navegador y si usted no dispone de esa clave no podrá exportar su certificado. Extraer la clave privada

Antes de leer este párrafo le recomendamos visite la sección de utilidades de la pkIRISGrid. Puede usar el programa pkcs12toglobus.sh para realizar estos pasos de forma automática.

Para este paso usted necesita openssl o alguna otra herramienta como grid-pkcs12

Si usa openssl para convertir el fichero al formato PEM: (reemplace irisgrid-cert-backup.p12 o irisgrid-cert-backup.pfx por el nombre de su fichero exportado)

> openssl pkcs12 -in irisgrid-cert-backup.p12 -out blah.pem -clcerts

Enter Import Password: MAC verified OK Enter PEM pass phrase: Verifying password - Enter PEM pass phrase:

Ahora el fichero PEM mantiene su certificado y su clave privada. Necesita separarlos en dos ficheros de la siguiente forma

cp blah.pem usercert.pem cp blah.pem userkey.pem

En el fichero con su certificado debe borrar la sección que habla de la clave privada. Para ello debe eliminar las líneas entre ---- BEGIN RSA PRIVATE KEY ---- y ---- END RSA PRIVATE KEY ----

En el fichero userkey.pem borre todo salvo lo contenido entre esas dos líneas. Debe quedarse también con las dos líneas

Ahora debe asegurarse de que nadie va a tener acceso a esos ficheros. Para ello basta con cambiar los permisos de los mismos

> chmod 0400 userkey.pem chmod 0444 usercert.pem

Para comprobar si todo ha ido bien puede probar con el comando grid-proxy-init en el directorio temporal actual

> grid-proxy-init -certdir .

Enter PEM pass phrase: ..+++++ .....+++++

> grid-proxy-info -all

subject : /DC=es/DC=irisgrid/CN=prueba@? issuer : /DC=es/DC=irisgrid/CN=CA type : full strength : 512 bits timeleft : 11:59:55

Si esto ha funcionado puede mover los dos ficheros a su directorio ~/.globus

ANTENCION: Si usted ya tenía credenciales válidas en su directorio .globus (por ejemplo de otra CA), sálvela primero en otra localización Instalar su certificado de usuario y probar IRISGrid

Debe configurar su entorno en su fichero de configuración .profile mediante la variable GLOBUS_LOCATION=/usr/local/globus y ejecutando el script /usr/local/globus/etc/globus-user-env.sh. Por ejemplo:

$ export GLOBUS_LOCATION=/usr/local/globus $ source /usr/local/globus/etc/globus-user-env.sh

Una vez que estas variables han sido tomadas por su entorno usted puede crear un certificado proxy que actúe como un punto único de autenticación para IRISGrid. Para ello ejecute:

$ grid-proxy-init

Copie el Nombre distintivo asociado al subject que le devuelve el comando grid-proxy-init y pidale a su administrador de globus que añada ese identificador al fichero gridmap al que usted tenga derecho