

Iniciación a las tecnologías Grid

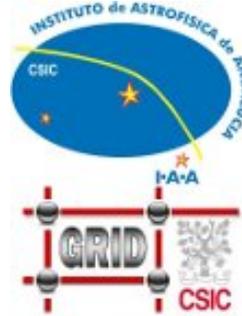
Granada. 8-12 de Marzo, 2010

<ftp://ftp.iaa.es/pub/sse/>

Susana Sánchez

Instituto de Astrofísica de Andalucía (IAA-CSIC)

sse@iaa.es



Tema 7: Pasos previos para el acceso al Grid

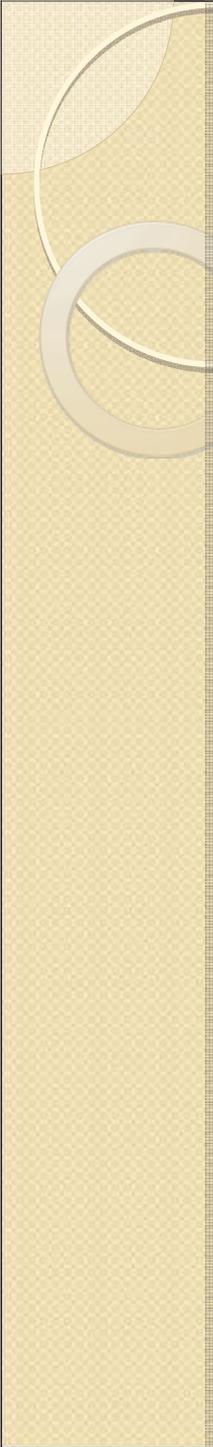
Susana Sánchez

Instituto de Astrofísica de Andalucía (IAA-CSIC)



Índice.

1. **Solicitud de un certificado digital**
 1. Certificados X.509
 2. Cómo solicitar el certificado
 3. Cómo Obtener el certificado
 4. Cómo renovar el certificado
2. **Cómo registrarse en una VO**
3. **Cómo crear la cuenta de usuario**
 1. La interfaz de Usuario
 2. Cómo verificar un certificado
4. **Certificados Proxy**
 1. Certificados proxy
 2. Servicio de membresía de la VO (VOMS)
 3. Renovación del proxy



Índice.

1. Solicitud de un certificado digital

1. Certificados X.509
2. Cómo solicitar el certificado
3. Cómo Obtener el certificado
4. Cómo renovar el certificado

2. Cómo registrarse en una VO

3. Cómo crear la cuenta de usuario

1. La interfaz de Usuario
2. Cómo verificar un certificado

4. Certificados Proxy

1. Certificados proxy
2. Servicio de membresía de la VO (VOMS)
3. Renovación del proxy

1.- Solicitud de un certificado digital

- Análogo al certificado de la FNMT
- Certificado X509 de una CA acreditada por EUGridPMA
- pkIRISGrid es la CA reconocida por EUGridPMA en España
- DN de un certificado:

/DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez

Domain Component

Common name

Organisation

1.- Solicitud de un certificado digital

<http://www.irisgrid.es/pki>

Elección de la Autoridad de Registro

A continuación mostramos un listado de las autoridades de registro disponibles junto con los espacios de nombre que gestionan. También puede verlas distribuidas en el [mapa de RAs de pkiRISGrid CA de España](#)

Institución	Espacio de nombres	RDN	Acceso RA	Responsable	Política RA
BSC/CNS	bsc.es deisa.bsc.es	O=bsc-cns O=deisa-bsc-cns	4	Juan Carlos Sanchez Del Barrio Javier Bartolomé	1.0.0
CESGA	cesga.es	O=cesga	8	Javier López Cacheiro	1.3.0
CICA	cica.es	O=cica	17	Sebastián Balboa García	En revisión
CIEMAT	ciemat.es eu-eela.org	O=ciemat O=eu-eela	12	Antonio Mollinedo	-
CIEMAT - CETA	ceta-ciemat.es	O=ceta-ciemat	13	Javier Perez-Griffo Callejon	-
CSIC	cenquior.csic.es	O=cenquior-csic	22	Aurelio Herrero Octavio Díaz-Pines Guillermo del Río	1.0.0
	cetef.csic.es	O=cetef-csic			
	cfmac.csic.es	O=cfmac-csic			
	cib.csic.es	O=cib-csic			
	cti.csic.es	O=cti-csic			
	ia.csic.es	O=acustica-csic			
	iai.csic.es	O=automatica-csic			
	icmm.csic.es	O=icmm-csic			
	icp.csic.es	O=icp-csic			
	ictp.csic.es	O=ictp-csic			
	iem.csic.es	O=iem-csic			
	ifa.csic.es	O=ifa-csic			
	ifi.csic.es	O=ifi-csic			
	imaff.csic.es	O=imaff-csic			
	inrc.csic.es	O=inrc-csic			
io.csic.es	O=optica-csic				
iqfr.csic.es	O=iqfr-csic				
iqm.csic.es	O=iqm-csic				
lqo.csic.es	O=lqo-csic				
mncn.csic.es	O=mncn-csic				
CSIC - CNB	cnb.csic.es	O=cnb-csic	26	Jose R. Valverde	-
DIPC	sw.ehu.es	O=dipc	21	Txomin Romero Asturiano	3.1.0
EHU	ehu.es	O=ehu	33	Juan Carlos Varona Herrera Juan Carlos Cuesta Medina	En revisión
ESA	esac.esa.int sciops.esa.int	O=esac-esa O=sciops-esa	15	Christophe Ariset	En revisión
I2BASK	i2bask.es	O=i2bask	24	Fco. Javier Ridruejo Pérez José Manuel Pérez Fuente	-
IAA	iaa.es	O=iaa	11	José Ruedas Sánchez	-

1.- Solicitud de un certificado digital

Selección de la RA correspondiente a nuestro dominio

ESA	esac.esa.int sciops.esa.int	O=esac-esa O=sciops-esa	15	Rubén Álvarez Fernando Félix Daniel Tapiador Adolfo Vázquez	1.1.0	✓ OK - 20091116
I2BASK	i2bask.es	O=i2bask	24	Rosario Sánchez Ojeda José Manuel Pérez Fuente	1.0.0	✓ OK - 20091113
IAA	iaa.es iaa.csic.es eea.csic.es eez.csic.es ipb.csic.es	O=iaa O=iaa O=eea O=eez O=ipb	11	José Ruedas Sánchez Benigno Cantero Rus Rafael Parra Garófano	1.0.0	✓ OK - 20090608
IAC	iac.es	O=iac	40	Diego Sierra Ubay Dorta Jorge Goya Antonio Díaz	1.0.0	✓ OK - 20090804
IFCA	ifca.es ifca.unican.es	O=ifca	25	Rafael Marco de Lucas	1.0.0	✓ OK - 20091216
IFIC	ific.uv.es	O=ific	23	Javier Sánchez Martínez	1.0.0	✓ OK - 20091215
PIC	ifae.es pic.es	O=ifae O=pic	2	Manuel Delfino	1.0.0	✓ OK - 20090511
RedIRIS	rediris.es irisgrid.es	O=rediris	1	Javier Masa Daniel García	1.1.0	✓ OK - 20090302
RedIRIS-test	test.rediris.es devel.rediris.es	O=test-rediris O=devel-rediris	1	Javier Masa Daniel García	1.0.1	✓ OK - 20090122

1.- Solicitud de un certificado digital

Seguir las instrucciones del formulario

- Identificador irisGrid: Código que identifica al usuario (ej: susana.sanchez@iaa.es)
- Clave usuario: Asociado al usuario. Servirá para comprobar la autoría de la solicitud ante la RA
- PIN: Asociado al certificado.

Identificador IRISGrid nombre.apellido @ iaa.es

Atención: Para usuarios del EGEE/LCG Grid es necesario usar un CN con (-) en lugar de (.) Tendrán que especificar [Nombre-Apellido]

Nombre

Apellidos

Clave de Usuario

Teléfono

email

PIN para certificado

Repite PIN

Privacidad ¿Desea incluir su email en el certificado? No Si
(en el campo X509v3 Subject Alternative Name)



1.- Solicitud de un certificado digital

Seguir las instrucciones del formulario

- Guardar los datos que se le muestra al enviar el formulario, ya que deberá presentarlos ante la autoridad de registro cuando verifique su identidad.
- Al confirmar los datos que se le muestra se generará un par de claves, quedando la privada guardada en el navegador, por lo que es imprescindible que cuando descargue el certificado sea mediante el mismo navegador con el que lo solicitó.
- Cuando la autoridad de registro verifique su identidad, enviará la solicitud a la CA, quien emitirá el certificado.
- Recibirá un e-mail indicándole los pasos para descargar el certificado.
- Mas información en

<http://www.irisgrid.es/pki/doc/pkirisgrid-ra-operation-visualguide-0.2.0.pdf>



1.- Solicitud de un certificado digital

RA en el IAA

- Personal encargado: José Ruedas, Rafa Parra, Benigno Cantero
- Dominios: iaa.csic.es, eez.csic.es, ipb.csic.es, eea.csic.es
- Normas: <http://www.irisgrid.es/pki/policy/ra/pkirisgrid-iaa-policy-1.0.0-20090608.pdf>
 - Documento de identificación (DNI, Pasaporte, NIE)
 - Documento acreditativo de vinculación laboral del centro emitido por la gerencia del mismo
 - Formulario cumplimentado
 - Reunión personal



1.- Solicitud de un certificado digital

Mi dominio no dispone de una RA

- Solicitar al propietario de su dominio la creación de una RA
- Cómo crear una RA:

<http://www.irisgrid.es/pki/ra/>

1.- Solicitud de un certificado digital

Cómo obtener el certificado

- Aprobada la solicitud se envía un mail al usuario
- Descargar del certificado DESDE EL MISMO NAVEGADOR
- El certificado queda instalado en el navegador
- Se puede obtener haciendo un backup del mismo (formato pkcs12)

Cómo Renovar el certificado

- Duración limitada del certificado (1 año)
- Solicitar la renovación desde un navegador con el certificado instalado.
- Desde el formulario web de la RA
- Durante un determinado tiempo previo a la expiración del mismo (el usuario es avisado)
- Se mantendrá el mismo DN del certificado

Índice.

1. Solicitud de un certificado digital

1. Certificados X.509
2. Cómo solicitar el certificado
3. Cómo Obtener el certificado
4. Cómo renovar el certificado

2. Cómo registrarse en una VO

3. Cómo crear la cuenta de usuario

1. La interfaz de Usuario
2. Cómo verificar un certificado

4. Certificados Proxy

1. Certificados proxy
2. Servicio de membresía de la VO (VOMS)
3. Renovación del proxy

1.- Cómo registrarse en una VO

En EGEE

- Registrarse en una VO ya creada.
 - Listado en <http://cic.in2p3.fr>
- Crear una VO propia
 - Contactar con un site que disponga de un servidor VOMS
 - Solicitar el alta de la VO en la infraestructura. Ver instrucciones en <http://cic.in2p3.fr>

En NGI

- Ya existen VO de la NGI.
- Se soportarán las VO de EGEE?
- Cuál será el procedimiento para aceptar nuevas VO?

1.- Cómo registrarse en una VO

VO creadas en NGI

vo.operaciones.es-ngi.eu

vo.general.es-ngi.eu

vo.formacion.es-ngi.eu

vo.grid4build.es-ngi.eu

vo.nanodev.es-ngi.eu

vo.mosfet.es-ngi.eu

vo.archist.es-ngi.eu

vo.blast.es-ngi.eu

vo.slgrid.es-ngi.eu

vo.photonics.es-ngi.eu

vo.qcomp.es-ngi.eu

vo.frodock.es-ngi.eu

vo.odthpiv.es-ngi.eu

vo.filogen.es-ngi.eu

vo.timones.es-ngi.eu

vo.gphase.es-ngi.eu

vo.turbulencia.es-ngi.eu

vo.meteo.es-ngi.eu



www.e-ciencia.es/wiki

vo.e-ca.es



<http://e-ca.iaa.es/php/224-organizacion-virtual-eca.htm>

- VO perteneciente a la infraestructura EGEE
- Soportada:
 - nodo GRID-CSIC del IAA
 - nodo e-ca-iaa
- Cualquier investigador perteneciente a una institución andaluza
- Objetivo: Facilitar el acceso a la infraestructura Grid
- Formulario de registro:

<https://swevo.ific.uv.es:8443/voms/vo.e-ca.es>

Índice.

1. Solicitud de un certificado digital

1. Certificados X.509
2. Cómo solicitar el certificado
3. Cómo Obtener el certificado
4. Cómo renovar el certificado

2. Cómo registrarse en una VO

3. Cómo crear la cuenta de usuario

1. La interfaz de Usuario
2. Cómo verificar un certificado

4. Certificados Proxy

1. Certificados proxy
2. Servicio de membresía de la VO (VOMS)
3. Renovación del proxy

3.- Cómo crear la cuenta de usuario

La interfaz del usuario

- SSH a la cuenta proporcionada por el administrador del UI.
- Crear el directorio \$HOME/.globus
- Instalar en ese directorio el certificado de usuario

```
[sse@ui ~]$ ls -la .globus/  
total 32  
drwxr-xr-x  3 sse sse 4096 Feb 25 11:06 .  
drwx----- 14 sse sse 4096 Feb 26 12:19 ..  
-r--r--r--  1 sse sse 2450 Feb 16 12:13 usercert.pem  
-r-----  1 sse sse 1914 Feb 16 12:13 userkey.pem
```

Generación de usercert.pem y userkey.pem a partir de un PKCS12

- Descargar el script [pkcs12toglobus.sh](http://www.irisgrid.es/pki/software/pkcs12toglobus.sh) de

<http://www.irisgrid.es/pki/software/pkcs12toglobus.sh>

```
[sse@ui ~]$ ./pkcs12toglobus.sh certificado.p12
```

3.- Cómo crear la cuenta de usuario

Verificar el certificado

```
[sse@ui ~]$ grid-cert-info
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 3036 (0xbdc)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: DC=es, DC=irisgrid, CN=IRISGridCA
    Validity
      Not Before: Aug 10 11:33:54 2009 GMT
      Not After : Aug 10 11:33:54 2010 GMT
    Subject: DC=es, DC=irisgrid, O=iaa, CN=susana.sanchez
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
      Modulus (2048 bit):
```

.....

Índice.

1. Solicitud de un certificado digital

1. Certificados X.509
2. Cómo solicitar el certificado
3. Cómo Obtener el certificado
4. Cómo renovar el certificado

2. Cómo registrarse en una VO

3. Cómo crear la cuenta de usuario

1. La interfaz de Usuario
2. Cómo verificar un certificado

4. Certificados Proxy

1. Certificados proxy
2. Servicio de membresía de la VO (VOMS)
3. Renovación del proxy



4.- Certificados Proxy

- Proxy = Credencial de usuario
- Necesario tener un proxy creado para la interacción con el Grid
- Proporciona seguridad:
 - Evita comprometer el certificado de usuario
 - Evita tener que dar la clave del certificado cada vez
 - Duración limitada (12 horas)

4.- Certificados Proxy

Creación de un Proxy

```
[sse@ui ~]$ grid-proxy-init
Your identity: /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
Enter GRID pass phrase for this identity:
Creating proxy
..... Done
Your proxy is valid until: Wed Mar  3 22:43:12 2010
```

Información de un proxy

```
[sse@ui ~]$ grid-proxy-info
subject  : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez/CN=934930265
issuer   : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
identity : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
type     : Proxy draft (pre-RFC) compliant impersonation proxy
strength : 512 bits
path     : /tmp/x509up_u501
timeleft : 11:56:43
```

Destrucción de un proxy

```
[sse@ui ~]$ grid-proxy-destroy
[sse@ui ~]$
```

4.- Certificados Proxy

Servicio de Membresía de la Organización Virtual (VOMS)

-Añade información sobre la VO del usuario al proxy

Crear un proxy del VOMS

```
[sse@ui ~]$ voms-proxy-init --voms vo.formacion.es-ngi.eu
Cannot find file or dir: /home/users/sse/.glite/vomses
Enter GRID pass phrase:
Your identity: /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
Creating temporary proxy ..... Done
Contacting voms01.ifca.es:15004
[/DC=es/DC=irisgrid/O=ifca/CN=host/voms01.ifca.es] "vo.formacion.es-
ngi.eu" Done
Creating proxy ..... Done
Your proxy is valid until Wed Mar  3 22:54:55 2010
```

4.- Certificados Proxy

Información de un proxy del VOMS

```
[sse@ui ~]$ voms-proxy-info --all
subject   : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez/CN=proxy
issuer    : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
identity  : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
type      : proxy
strength  : 1024 bits
path      : /tmp/x509up_u501
timeleft  : 11:58:25
=== VO vo.e-ca.es extension information ===
VO        : vo.e-ca.es
subject   : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
issuer    : /DC=es/DC=irisgrid/O=ific/CN=swevo.ific.uv.es
attribute : /vo.e-ca.es/Role=NULL/Capability=NULL
timeleft  : 11:58:25
uri       : swevo.ific.uv.es:14005
```

Eliminar un proxy del VOMS

```
[sse@ui ~]$ voms-proxy-destroy
```



4.- Renovación del proxy

- Problema: duración proxy < duración trabajo
- Solución mala: Crear proxy de mayor duración
 - Mayor riesgo de seguridad
 - Los servidores VOMS no permiten crear proxy > 24h
- Solución buena: Uso de servidores MyProxy
 - Se almacena un proxy de larga duración en el servidor (1 semana)
 - A partir de éste se obtiene un certificado de corta duración (12 horas)
 - El certificado de corta duración se va renovando

4.- Certificados Proxy

Creación de un proxy de larga duración

```
[sse@ui ~]$ myproxy-init
Your identity: /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
Enter GRID pass phrase for this identity:
Creating proxy .....
Done
Proxy Verify OK
Your proxy is valid until: Wed Mar 10 11:16:24 2010
Enter MyProxy pass phrase:
Verifying - Enter MyProxy pass phrase:
A proxy valid for 168 hours (7.0 days) for user sse now exists on
gridpx01.ifca.es.
```

-Se introducen dos claves:

- La clave del certificado
- La clave con la que se guardará el proxy en el servidor (necesaria para delegación)

4.- Certificados Proxy

Información de un proxy de larga duración

```
[sse@ui ~]$ myproxy-info
username: sse
owner: /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
timeleft: 166:44:19 (6.9 days)
```

Ojo: Si solo hemos creado el proxy en el servidor obtendremos un error. Previamente debemos obtener una delegación. Tampoco funcionara grid-proxy-info

Obtener una delegación

```
[sse@ui ~]$ myproxy-get-delegation
```

Enter MyProxy pass phrase:

A credential has been received for user sse in /tmp/x509up_u501.

Probad ahora grid-proxy-info!

Destruir un proxy de larga duración

```
[sse@ui ~]$ myproxy-destroy
```

Default MyProxy credential for user sse was successfully removed.



Tras destruir el proxy en el servidor MyProxy, ejecutad
grid-proxy-info

```
[sse@ui ~]$ grid-proxy-info
subject   : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez/CN=934930265
issuer    : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
identity  : /DC=es/DC=irisgrid/O=iaa/CN=susana.sanchez
type      : Proxy draft (pre-RFC) compliant impersonation proxy
strength  : 512 bits
path      : /tmp/x509up_u501
timeleft  : 11:56:43
```

¿Por qué seguimos teniendo un proxy?

- **BUG conocido: añadir la extension VOMS al myproxy**
- http://cds.u-strasbg.fr/twikiDCA/bin/view/EuroVODCA/AuthenticationAuthorization#The_use_of_myproxy