



# Sistemas Grid Basados en GT3



## Módulo 4 Seguridad en GT3

*Borja Sotomayor*  
5 de marzo de 2004



# Introducción

- ▶ En este módulo aprenderemos a trabajar con los servicios de seguridad de GT3, basados en el Grid Security Infrastructure (GSI)
- ▶ Añadiremos diferentes modalidades de seguridad a MathService.



## Índice

- ▶ GSI: Grid Security Infrastructure
- ▶ Configuración de GSI
- ▶ Un Grid Service con Seguridad
- ▶ El Fichero de Configuración de Seguridad
- ▶ Autorización Mediante Gridmaps
- ▶ Delegación de Credenciales

Sistemas Grid Basados en GT3



## Índice

- ▶ GSI: Grid Security Infrastructure
- ▶ Configuración de GSI
- ▶ Un Grid Service con Seguridad
- ▶ El Fichero de Configuración de Seguridad
- ▶ Autorización Mediante Gridmaps
- ▶ Delegación de Credenciales

Sistemas Grid Basados en GT3



## GSI (I)

- ▶ La seguridad es muy importante en aplicaciones Grid.
  - ▶ Entorno heterogéneo en el que intervienen múltiples organizaciones con distintas políticas de seguridad.
- ▶ GT3 afronta los desafíos de seguridad con el GSI – Grid Security Infrastructure.



## GSI (II)

- ▶ GSI (también llamado “los servicios de seguridad”) ofrece lo siguiente:
  - ▶ Un sistema de criptografía de llave pública (public key system)
  - ▶ Autenticación mutua mediante certificados x509
  - ▶ Delegación de credenciales y “single sign-on”
- ▶ GSI se compone de:
  - ▶ Comandos para gestionar certificados.
  - ▶ Clases Java para integrar (y configurar) la seguridad en los grid services y en sus clientes.



## Delegación y Single Sign-on (I)

- ▶ En aplicaciones Grid es habitual *delegar* credenciales para que un nodo pueda actuar en nombre de otro nodo.
- ▶ Esto se consigue mediante *certificados proxy*.
  - ▶ Certificado x509 especial firmado por un usuario final en lugar de una CA.
  - ▶ Autoriza al portador del proxy a actuar en nombre del usuario que lo ha firmado.
  - ▶ Tienen duración y funcionalidad limitada.



## Delegación y Single Sign-on (II)

- ▶ Como consecuencia de la delegación, también conseguimos “single sign-on”
  - ▶ Sin delegación, tendría que autenticarme con todas las organizaciones con las que voy a interactuar en la aplicación. Cada vez que me autentico, debo acceder a mi clave privada: multiple sign-on.
  - ▶ Con delegación, utilizo un proxy certificate para permitir que un nodo actúe en mi nombre. Sólo accedo a mi clave privada para firmar el proxy certificate: single sign-on



## Índice

- ▶ GSI: Grid Security Infrastructure
- ▶ **Configuración de GSI**
- ▶ Un Grid Service con Seguridad
- ▶ El Fichero de Configuración de Seguridad
- ▶ Autorización Mediante Gridmaps
- ▶ Delegación de Credenciales



## Configuración de GSI (I)

- ▶ La configuración de GSI básicamente se reduce a conseguir uno o varios certificados digitales para nuestra máquina.
- ▶ Podemos tener múltiples certificados:
  - ▶ Para usuarios individuales.
  - ▶ Para la máquina (*host certificate*)
  - ▶ Para un servicio concreto
- ▶ En nuestro caso, necesitamos un certificado para el usuario globus y otro para nuestro usuario.



## Configuración de GSI (II)

- ▶ Para obtener un certificado tenemos que:
  - ▶ Conseguir el certificado del CA al que queremos solicitar un certificado.
  - ▶ Generar una petición de certificado.
  - ▶ Enviársela al CA.
  - ▶ El CA nos devolverá el certificado firmado.
  - ▶ Instalar el certificado.



## Configuración de GSI (III)

- ▶ Como no tenemos un CA a mano...
  - ▶ Los ejemplos incluyen ya los certificados para el usuario globus y para nuestro usuario.
  - ▶ También se incluye el certificado del CA que ha expedido los certificados, para que GSI pueda verificar la autenticidad de los certificados.
  - ▶ Usuario globus
    - ▶ \$TUTORIAL\_DIR/certificates.globus
  - ▶ Usuario normal
    - ▶ \$TUTORIAL\_DIR/certificates.usuario



## Configuración de GSI (IV)

- ▶ Contenidos de `certificates.globus` y `certificates.usuario`:
  - ▶ `usercert.pem`: Certificado digital del usuario
  - ▶ `userkey.pem`: Clave privada del usuario
  - ▶ `certificates/24d355a5.0`: Certificado del CA
  - ▶ `certificates/24d355a5.signing_policy`: Política de firma del CA.



## Configuración de GSI (V)

- ▶ Instalación de los certificados del usuario globus (desde directorio home de globus)

```
mkdir .globus
cp -r $TUTORIAL_DIR/certificates.globus/* .globus
chmod 400 .globus/userkey.pem
```

- ▶ Instalación de los certificados del usuario normal (desde su directorio home)

```
mkdir .globus
cp -r $TUTORIAL_DIR/certificates.usuario/* .globus
chmod 400 .globus/userkey.pem
```



## Comandos Útiles (I)

### ► Creación del certificado proxy:

```
java org.globus.tools.ProxyInit
```

- Ejecutar este comando desde ambas cuentas
- Esto nos permitirá comprobar si los certificados están correctamente instalados
- El certificado proxy se crea en /tmp y tiene como nombre x509up\_u<UID del usuario>



## Comandos Útiles (II)

### ► Para ver la información de un certificado:

```
java org.globus.tools.CertInfo -file <fichero certificado>
```

- Ejecutar este comando desde ambas cuentas
- Esto nos permitirá comprobar si los certificados están correctamente instalados
- El certificado proxy se crea en /tmp y tiene como nombre x509up\_u<UID del usuario>



## Comandos Útiles (III)

- ▶ Estamos utilizando la versión Java de estos comandos porque estamos utilizando sólo el núcleo de GT3.
- ▶ La versión completa incluye los comandos *grid-proxy-init* y *grid-cert-info*.



## Configuración de GSI

- ▶ Guías de instalación que abordan la instalación y configuración de GSI:
  - ▶ “GT3 Quick Start” (Redpaper de IBM)  
<http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp3697>  
(o sencillamente “GT3 Quick Start Redpaper” en Google)
  - ▶ From Zero to GT3  
<http://www-pnp.physics.ox.ac.uk/~stokes/twiki/bin/view/DIRAC/GT3Express>
  - ▶ The Globus Toolkit 3 Programmer's Tutorial (con SimpleCA)  
<http://www.casa-sotomayor.net/gt3-tutorial/>



## Índice

- ▶ GSI: Grid Security Infrastructure
- ▶ Configuración de GSI
- ▶ **Un Grid Service con Seguridad**
- ▶ El Fichero de Configuración de Seguridad
- ▶ Autorización Mediante Gridmaps
- ▶ Delegación de Credenciales

Sistemas Grid Basados en GT3



## Añadir Seguridad a MathService

- ▶ **Vamos a añadir seguridad al MathService más básico (primer ejemplo de GT3 Core).**
  - ▶ Reutilizamos el interfaz (GWSDL)
    - ▶ `$TUTORIAL_DIR/schema/progtutorial/MathService/Math.gwsdl`
  - ▶ **Modificamos la implementación (Java)**
    - ▶ No es estrictamente necesario, pero vamos a escribir en consola datos de seguridad.
  - ▶ **Modificamos el despliegue (WSDD)**

Sistemas Grid Basados en GT3



## Implementación

### ► Implementación – Cambios

- \$TUTORIAL\_DIR/org/globus/progtutorial/services/security/first/impl/MathProvider.java
- Utilizamos `operation providers` en vez de heredar de `GridServiceImpl`.
- Añadimos un método privado llamado `logSecurityInfo` que muestra datos de seguridad
  - Identidad del cliente
  - Sujeto de invocación, servicio, y sistema.



## Descriptor de Despliegue

### ► Descriptor de despliegue

- Añadimos dos parámetros:

```
<parameter name="securityConfig"
value="org/globus/ogsa/impl/security/descriptor/gsi-
security-config.xml"/>
<parameter name="authorization" value="none"/>
```
- *securityConfig*: El fichero de configuración de seguridad, en el que se especifica qué métodos van a ser seguros, y con qué nivel de seguridad.
  - Utilizamos un fichero por defecto "Todos los métodos con seguridad"
- *authorization*: Método de autorización.



## Cliente

- ▶ Activar la seguridad en el cliente es bastante sencillo. Hay que modificar unas propiedades del stub.

```
((Stub)math)._setProperty(  
    Constants.GSI_SEC_CONV, Constants.ENCRYPTION  
);  
((Stub)math)._setProperty(  
    Constants.AUTHORIZATION, NoAuthorization.getInstance()  
);
```



## Activar Logging

- ▶ La implementación va a utilizar el API de logging, por lo que hay que activar el logging para MathService.
- ▶ Añadir al final de \$GLOBUS\_LOCATION/ogsilogging.properties:

```
org.globus.progtutorial.services.security.first.impl.  
MathProvider=console,debug
```

(todo en una línea)



## Compilar, Desplegar, Ejecutar

- ▶ Como usuario
  - ▶ `./tutorial_build.sh`  
`org.globus/progtutorial/services/security/first/  
schema/progtutorial/MathService/Math.gwsdl`
- ▶ Como globus
  - ▶ `ant deploy -Dgar.name=$TUTORIAL_DIR/build/lib/<gar>`
  - ▶ `globus-start-container`
- ▶ Como usuario
  - ▶ `javac -classpath ./build/classes/:$CLASSPATH  
org.globus/progtutorial/clients/MathService/ClientGSIConvEncrypt.java`
  - ▶ `java -classpath ./build/classes/:$CLASSPATH  
org.globus/progtutorial/clients/MathService/ClientGSIConvEncrypt  
http://127.0.0.1:8080/ogsa/services/progtutorial/security/first/MathService 5`



## Índice

- ▶ GSI: Grid Security Infrastructure
- ▶ Configuración de GSI
- ▶ Un Grid Service con Seguridad
- ▶ El Fichero de Configuración de Seguridad
- ▶ Autorización Mediante Gridmaps
- ▶ Delegación de Credenciales



## Fichero de Conf. de Seguridad (I)

- ▶ El fichero de configuración de seguridad nos permite controlar, método a método, lo siguiente:
  - ▶ El método de autenticación y su nivel de protección (encriptación, integridad, ...)
  - ▶ La identidad de ejecución del servicio (útil para delegación de credenciales)
- ▶ Es un fichero XML. Lo vinculamos a un servicio mediante el parámetro *securityConfig* del WSDD.



## Fichero de Conf. de Seguridad (II)

- ▶ Vamos a utilizar dos ficheros de configuración propios.
  - ▶ \$TUTORIAL\_DIR/org/globus/progtutorial/services/security/first/config/security-config-auth.xml  
Para probar distintos tipos de autenticación.
  - ▶ \$TUTORIAL\_DIR/org/globus/progtutorial/services/security/first/config/security-config-runas.xml  
Para probar distintas identidades de ejecución.
- ▶ No necesitamos volver a compilar y desplegar. Junto con el ejemplo anterior se desplegaron dos servicios con la misma implementación, pero utilizando cada uno de los ficheros de configuración.
- ▶ Utilizaremos nuevos clientes para probar las configuraciones.



## Tipos de Autenticación (I)

- ▶ Tipos de autenticación:
  - ▶ GSI Secure Conversation (<gsi> ... </gsi>)
    - ▶ Nivel de protección (<protection-level>...</protection-level> )
      - ▶ Privacy ( <privacy/> )
      - ▶ Integrity ( <integrity/> )
  - ▶ GSI Secure Message (<pkey/>)



## Tipos de Autenticación (II)

```
<securityConfig xmlns="http://www.globus.org"
  xmlns:math=
"http://www.globus.org/namespaces/2004/02/progtutorial/MathService">

<method name="math:add">
  <auth-method>
    <gsi>
      <protection-level>
        <integrity/>
        <privacy/>
      </protection-level>
    </gsi>
  </auth-method>
</method>

<!-- Otros metodos -->

</securityConfig>
```



## Tipos de Autenticación (III)

- ▶ Cliente con encriptación
  - ▶ `javac -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientGSICovEncrypt.java`
  - ▶ `java -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientGSICovEncrypt http://127.0.0.1:8080/ogsa/services/progtutorial/security/first/MathAuthService 5`
- ▶ Cliente con integridad
  - ▶ `javac -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientGSICovSigned.java`
  - ▶ `java -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientGSICovSigned http://127.0.0.1:8080/ogsa/services/progtutorial/security/first/MathAuthService 5`
- ▶ Cliente sin seguridad
  - ▶ `javac -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientNoSecurity.java`
  - ▶ `java -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientNoSecurity http://127.0.0.1:8080/ogsa/services/progtutorial/security/first/MathAuthService 5`

Sistemas Grid Basados en GT3



## Identidades de Ejecución (I)

- ▶ No veremos su aplicación práctica hasta que utilicemos delegación.
- ▶ Podemos especificar, método a método, la identidad que adoptará durante su ejecución:
  - ▶ Cliente (`<caller-identity />`)
  - ▶ Sistema (`<system-identity />`)
  - ▶ Servicio (`<service-identity />`)

Sistemas Grid Basados en GT3



## Identidades de Ejecución (II)

- ▶ La identidad concreta que se modifica es la *identidad de invocación*. El servicio siempre tiene otras dos identidades asociadas:
  - ▶ La identidad del sistema
  - ▶ La identidad del servicio (igual a la del sistema si no se han especificado credenciales para el servicio)



## Identidades de Ejecución (III)

```
<securityConfig xmlns="http://www.globus.org"
  xmlns:math=
"http://www.globus.org/namespaces/2004/02/progtutorial/MathService">
<method name="math:add">
  <run-as>
    <caller-identity/>
  </run-as>
</method>
<!-- otros metodos -->
</securityConfig>
```



## Identidades de Ejecución (IV)

### ▶ Como usuario

- ▶ `javac -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientGSIConvEncrypt.java`
- ▶ `java -classpath ./build/classes/:$CLASSPATH org/globus/progtutorial/clients/MathService/ClientGSIConvEncrypt http://127.0.0.1:8080/ogsa/services/progtutorial/security/first/MathRunAsService 5`



## Índice

- ▶ GSI: Grid Security Infrastructure
- ▶ Configuración de GSI
- ▶ Un Grid Service con Seguridad
- ▶ El Fichero de Configuración de Seguridad
- ▶ **Autorización Mediante Gridmaps**
- ▶ Delegación de Credenciales



## Métodos de Autorización

- ▶ GT3 soporta varios métodos de *autorización*.
  - ▶ En el lado del servidor:
    - ▶ None
    - ▶ Self
    - ▶ **Gridmap**
  - ▶ En el lado del cliente
    - ▶ None
    - ▶ Self
    - ▶ Host



## Gridmaps

- ▶ El gridmap es un ACL (Access Control List).
  - ▶ Contiene una lista de los usuarios que tienen permitido el acceso a un servicio concreto.
  - ▶ El gridmap contiene una lista de subjects (de los certificados digitales de los usuarios)
  - ▶ En los servicios de alto nivel, también realiza un mapeo a cuentas de usuario para lanzar procesos con esa cuenta de usuario.



## El Fichero gridmap

- ▶ Con la cuenta de globus crear un fichero `$GLOBUS_LOCATION/gridmap` con el siguiente contenido:

```
"/O=Globus/OU=GT3 Tutorial/CN=Usuario Tutorial" curso
```



## Descriptor de Despliegue

- ▶ Para añadir autorización mediante gridmap a un servicio, añadimos los siguientes parámetros en el WSDD:

```
<parameter name="gridmap" value="<path gridmap>"/>  
<parameter name="authorization" value="gridmap"/>
```



## Servicio con Gridmap (I)

- ▶ Vamos a desplegar un nuevo servicio con autorización gridmap.
- ▶ Podríamos reutilizar todo el código de los ejemplos anteriores (definiendo otro despliegue más), pero vamos a modificar la implementación de cara al siguiente ejercicio.
  - ▶ La información de seguridad que se escribe en consola va a ser más compacta.



## Servicio con Gridmap (II)

- ▶ Nuevo servicio
  - ▶ Reutilizamos interfaz (WSDL)
  - ▶ Modificamos implementación (Java)
    - ▶ `$TUTORIAL_DIR/org/globus/progtutorial/services/security/gridmap/impl/MathProvider.java`
    - ▶ Escribe menos información de seguridad
  - ▶ Modificamos despliegue (WSDD)
    - ▶ `$TUTORIAL_DIR/org/globus/progtutorial/services/security/gridmap/server-deploy.wsdd`
    - ▶ Añadimos parámetros para autorización gridmap



## Activar Logging

- ▶ Este nuevo servicio también utiliza la API de logging.
- ▶ Añadir al final de \$GLOBUS\_LOCATION/ogsilogging.properties:

```
org.globus.progtutorial.services.security.first.impl.  
MathProvider=console,debug
```

(todo en una linea)

Sistemas Grid Basados en GT3



## Compilar, Desplegar, Ejecutar

- ▶ Como usuario
  - ▶ ./tutorial\_build.sh  
org/globus/progtutorial/services/security/gridmap/  
schema/progtutorial/MathService/Math.gwsdl
- ▶ Como globus
  - ▶ ant deploy -Dgar.name=\$TUTORIAL\_DIR/build/lib/<gar>
  - ▶ globus-start-container
- ▶ Como usuario
  - ▶ javac -classpath ./build/classes/:\$CLASSPATH  
org/globus/progtutorial/clients/MathService/ClientGSIConvEncrypt.java
  - ▶ java -classpath ./build/classes/:\$CLASSPATH  
org/globus/progtutorial/clients/MathService/ClientGSIConvEncrypt  
http://127.0.0.1:8080/ogsa/services/progtutorial/security/gridmap/MathService 5
- ▶ Si ejecutamos el cliente con la cuenta globus, recibiremos un mensaje de error porque el usuario globus no está en el gridmap.

Sistemas Grid Basados en GT3



## Índice

- ▶ GSI: Grid Security Infrastructure
- ▶ Configuración de GSI
- ▶ Un Grid Service con Seguridad
- ▶ El Fichero de Configuración de Seguridad
- ▶ Autorización Mediante Gridmaps
- ▶ Delegación de Credenciales



## Delegación (I)

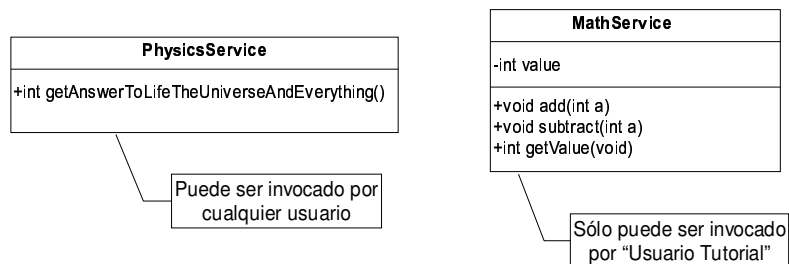
- ▶ Para este ejemplo vamos a utilizar el MathService con autorización gridmap y un nuevo servicio llamado PhysicsService.

PhysicsService
+int getAnswerToLifeTheUniverseAndEverything()



## Delegación (II)

- ▶ PhysicsService invoca el método add() de MathService.



## Delegación (III)

- ▶ PhysicsService se ejecuta bajo la identidad de "Administrador Globus" (el usuario globus que ejecuta el contenedor)
  - ▶ No puede invocar a MathService (no está autorizado en el gridmap)
- ▶ Solución: El usuario ("Usuario Tutorial") puede delegar sus credenciales a PhysicsService.
  - ▶ PhysicsService utilizará esas credenciales delegadas para invocar a MathService.



## Ejemplo (I)

- ▶ Vamos a ver dos PhysicsService
  - ▶ Sin delegación de credenciales
  - ▶ Con delegación de credenciales



## Ejemplo (II)

- ▶ El mismo interfaz para ambos ejemplos (GWSDL)
  - ▶ `$TUTORIAL_DIR/schema/progtutorial/PhysicsService/Physics.gwsdl`
- ▶ Implementación sin y con delegación
  - ▶ `$TUTORIAL_DIR/org/globus/progtutorial/services/security/delegation/impl/PhysicsProviderNoDelegation.java`
  - ▶ `$TUTORIAL_DIR/org/globus/progtutorial/services/security/delegation/impl/PhysicsProvider.java`
- ▶ El WSDD contiene la descripción de ambos servicios.
  - ▶ `$TUTORIAL_DIR/org/globus/progtutorial/services/security/delegation/server-deploy.wsdd`



## Ejemplo (III)

```
<securityConfig xmlns="http://www.globus.org"
  xmlns:physics=
"http://www.globus.org/namespaces/2004/02/progtutorial/PhysicsService">

<method name="physics:getAnswerToLifeTheUniverseAndEverything">
  <run-as>
    <caller-identity/>
  </run-as>
  <auth-method>
    <gsi/>
  </auth-method>
</method>

<auth-method>
  <gsi/>
</auth-method>

</securityConfig>
```

Sistemas Grid Basados en GT3



## Compilar y Desplegar

- ▶ Como usuario
  - ▶ ./tutorial\_build.sh  
org/globus/progtutorial/services/security/delegation/  
schema/progtutorial/MathService/Math.gwsdl
- ▶ Como globus
  - ▶ ant deploy -Dgar.name=\$TUTORIAL\_DIR/build/lib/<gar>
  - ▶ globus-start-container

Sistemas Grid Basados en GT3



## Cientes

### ▶ Cliente sin delegación:

```
▶ javac -classpath ./build/classes/.$CLASSPATH
org/globus/progtutorial/clients/PhysicsService/ClientNoDelegation.java
▶ java -classpath ./build/classes/.$CLASSPATH
org/globus/progtutorial/clients/PhysicsService/ClientNoDelegation
http://127.0.0.1:8080/ogsa/services/progtutorial/security/delegation/PhysicsService
```

### ▶ Cliente sin delegación:

```
▶ javac -classpath ./build/classes/.$CLASSPATH
org/globus/progtutorial/clients/PhysicsService/ClientDelegation.java
▶ java -classpath ./build/classes/.$CLASSPATH
org/globus/progtutorial/clients/PhysicsService/ClientDelegation
http://127.0.0.1:8080/ogsa/services/progtutorial/security/delegation/PhysicsService
```

## ¿Preguntas?



**Borja Sotomayor**  
Facultad de Ingeniería - ESIDE  
Universidad de Deusto  
[bsotomay@eside.deusto.es](mailto:bsotomay@eside.deusto.es)