



Enabling Grids for E-science

# A VO-Oriented AuthN/AuthZ Approach

*Vincenzo Ciaschini*

*EGEE 2<sup>nd</sup> User Forum*

*Manchester, 9-11 May, 2007*

[www.eu-egee.org](http://www.eu-egee.org)



## User AuthN/AuthZ management on the grid is rapidly changing and evolving

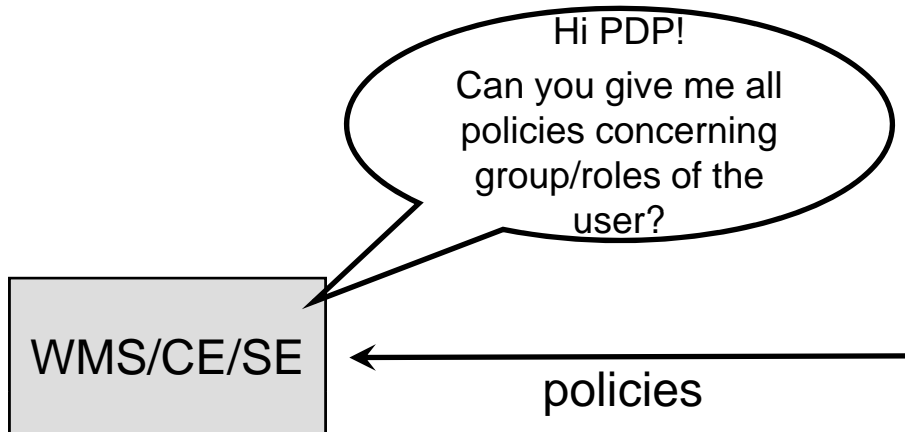
- VOs define/use/modify groups and roles.
- VOs require different execution priorities for different users.
- VOs require dedicated resources for specific users in delicate periods (see Data Challenges, etc.)
- funding agencies can force constraints affecting resource allocations.
- sites may want to enforce site-specific policies.

# An AuthN/AuthZ infrastructure



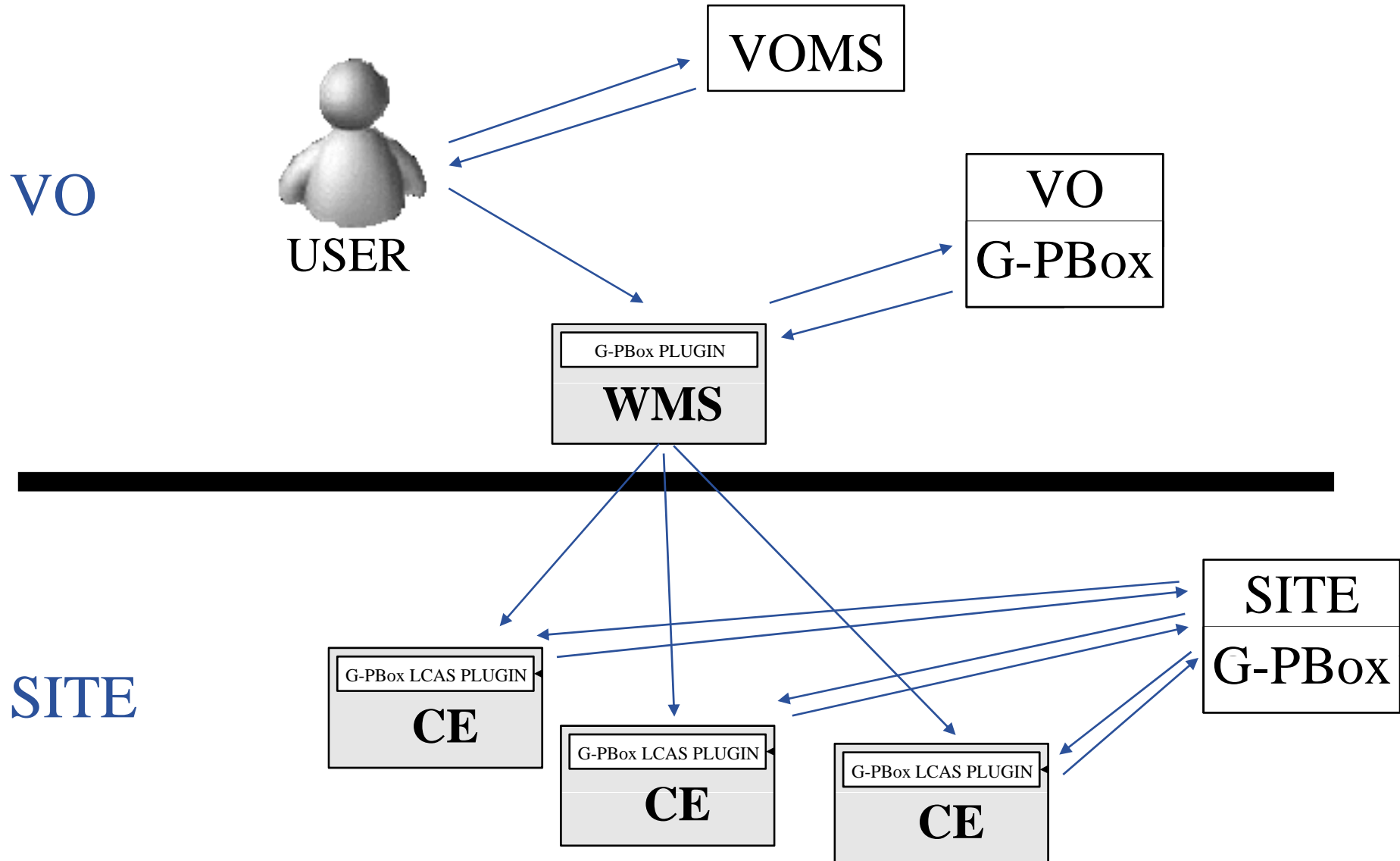
AA

USER	GROUP
O=INFN/CN=John Smith	/atlas/production
...	...



PDP

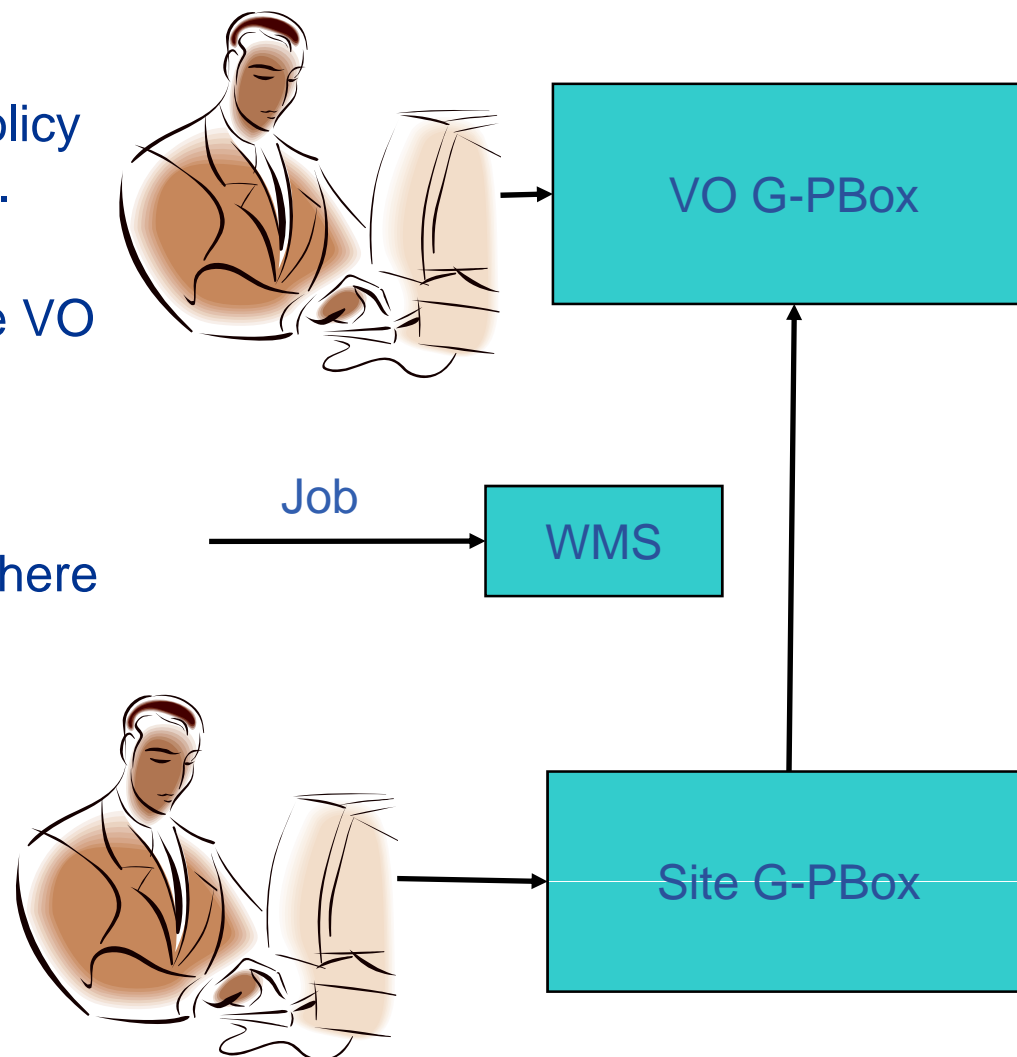
GROUP	WHERE	HOW	WHEN
/atlas/production	Tier1s	HIGH PRIORITY	May 2007
/atlas	Tier1s and Tier2s	MID PRIORITY	ANY
/atlas/students	Tier2s	LOW PRIORITY	ANY



- **Site policies (originated by sites)**
  - Ban-list
  - ...
- **VO policies (originated by VOs)**
  - Intra-VO priorities
  - ...

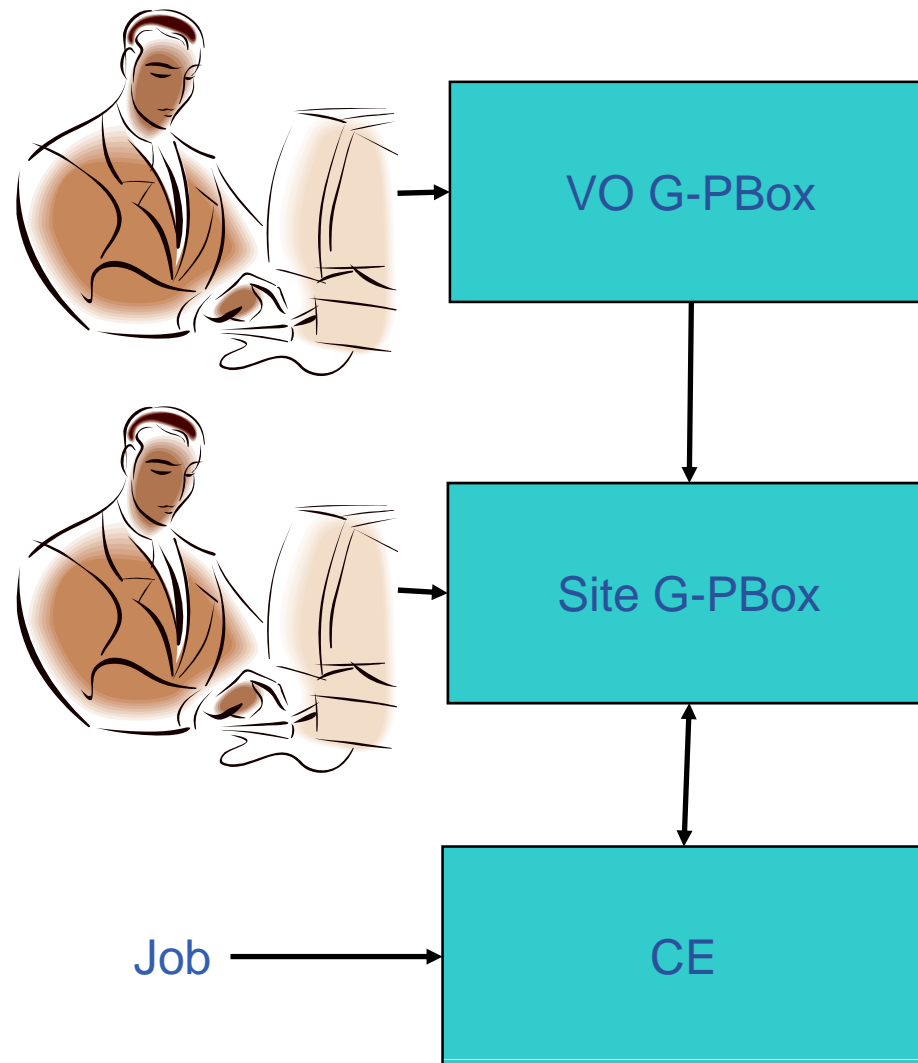
- **Banning users:**

- The site admin writes a policy banning a user or a group.
- The ban policy gets communicated back to the VO G-PBox.
- Whenever a job is sent to WMS, policy evaluation happens and resources where the user is banned do not receive the job.

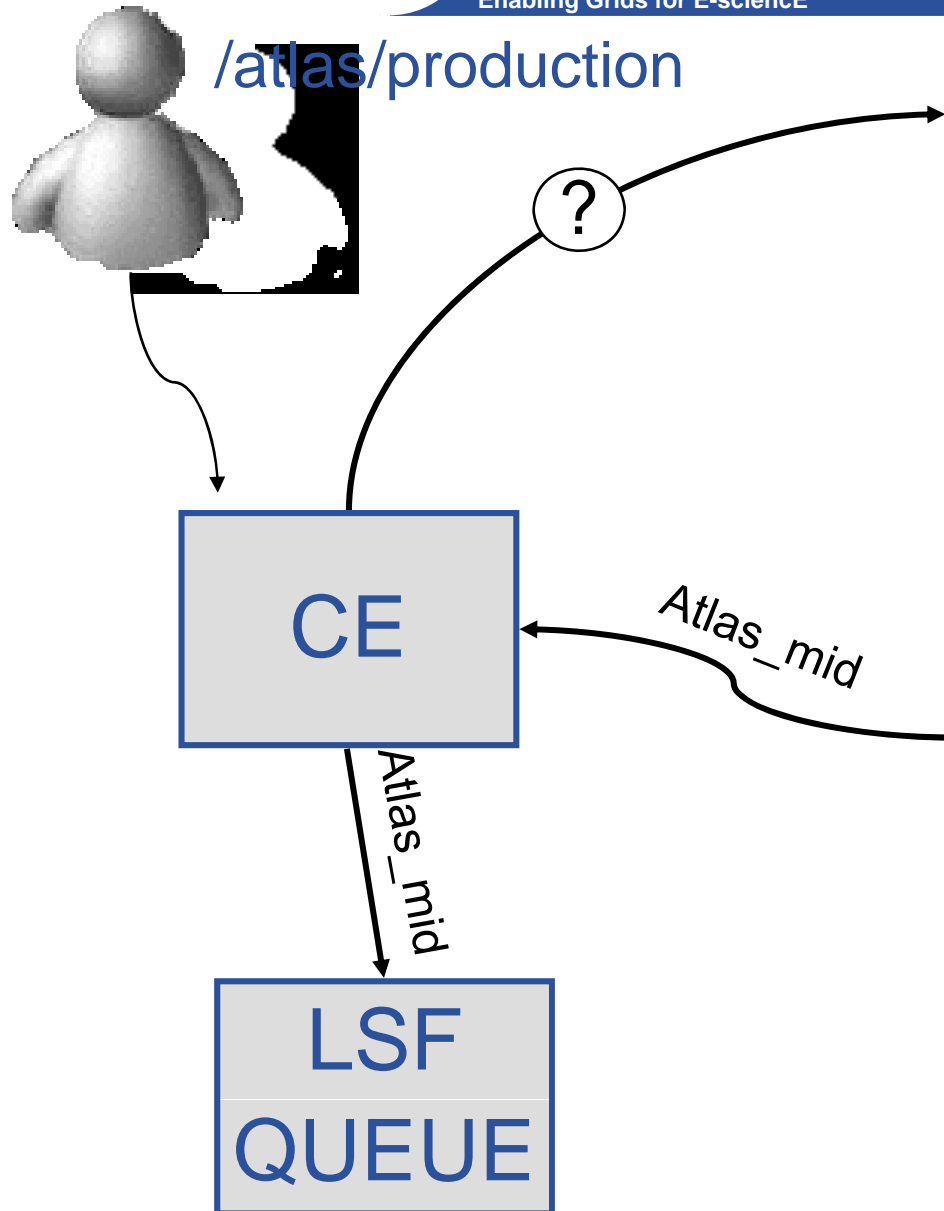


- **Step 1:**
  - Define a set of shares on CEs which implement the required priorities.
  - Publish into the IS the shares that are supported (without publishing details, i.e: policies, about how they are used).
  - This has already been solved and implemented!
- **Step 2:**
  - Send a Job to a CE which implements the correct share.
  - Let the CE map the job on the correct share.

- **Mapping jobs to shares: a G-PBox solution.**
  - The VO writes policies mapping VO groups into share names.
  - The sites write policies mapping share names into actual batch system shares.
  - The VO sends their mapping policies to the site. The two get combined.
  - Whenever a job is sent to a CE, evaluation happens and the job is mapped to the right account.



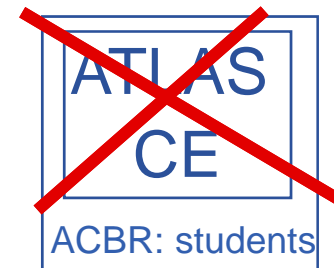
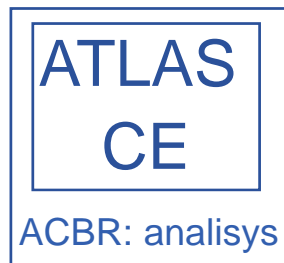
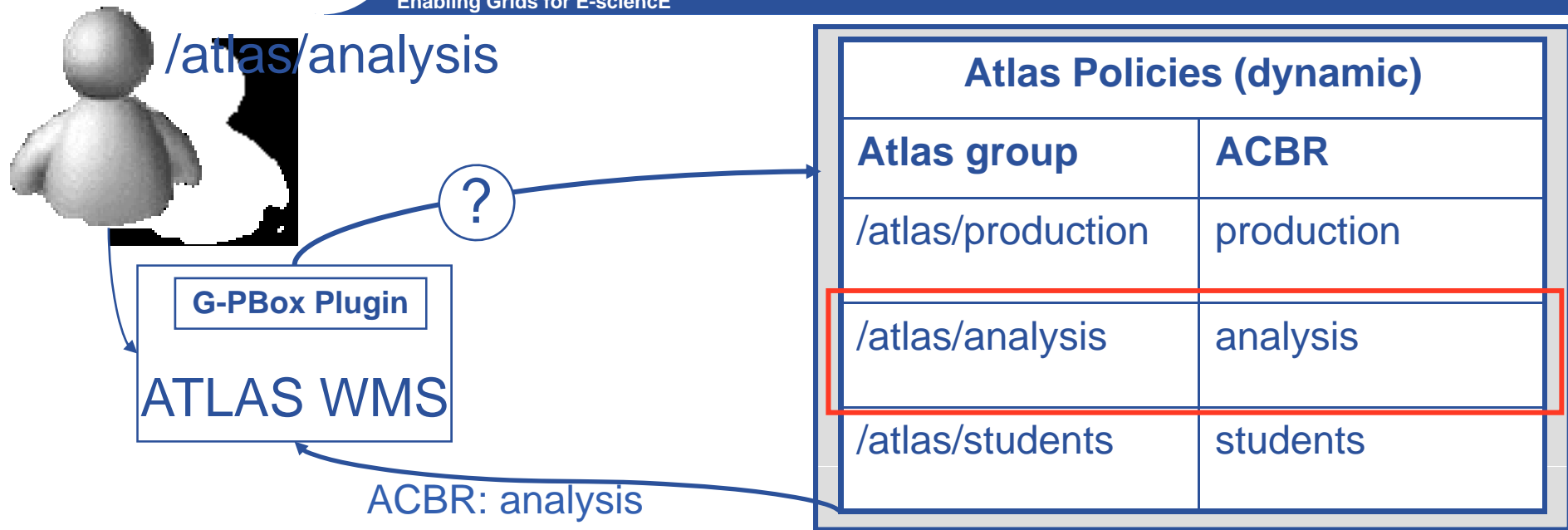




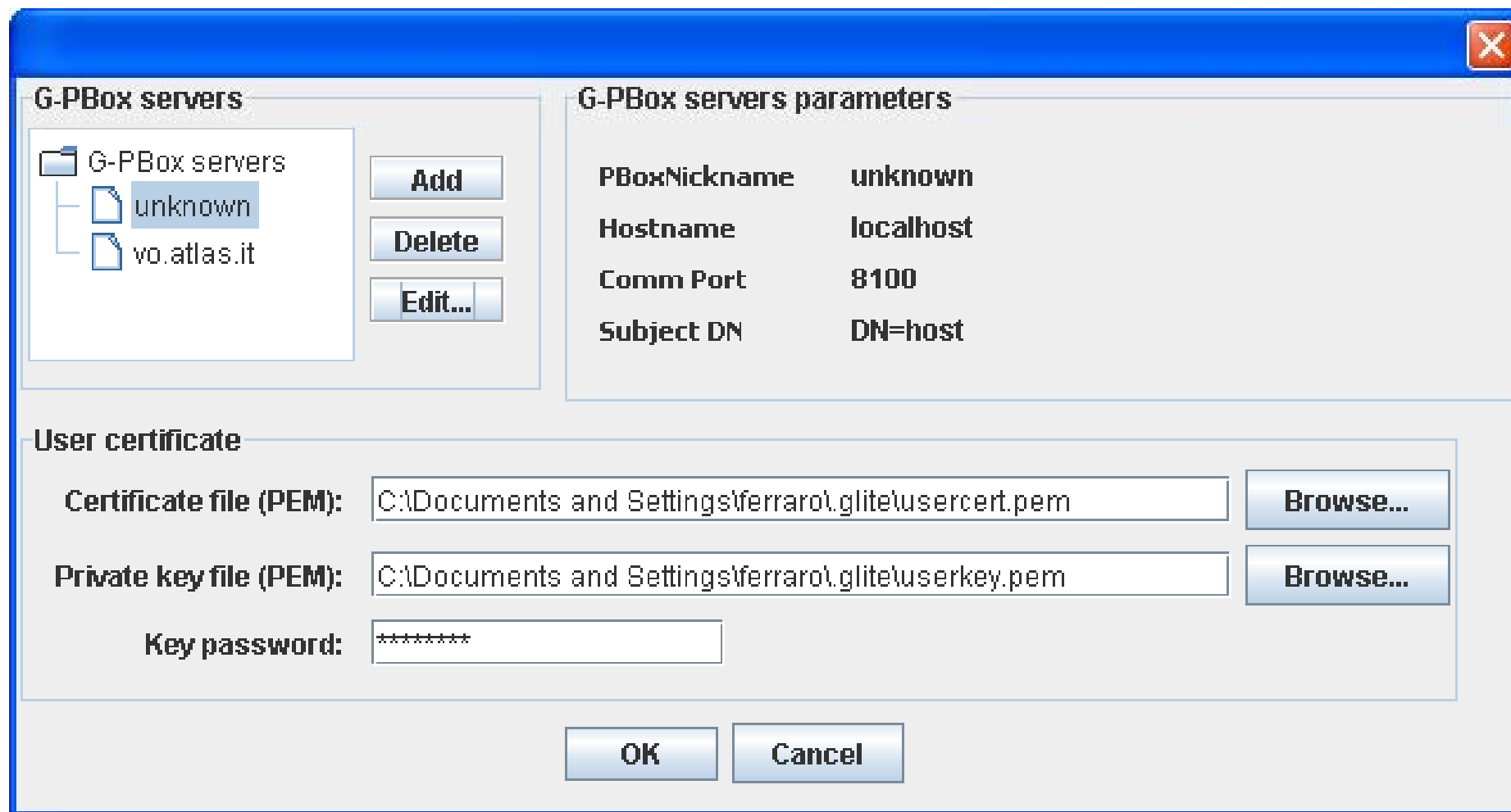
Atlas Policies (dynamic)	
<b>Atlas group</b>	<b>ACBR</b>
/atlas/production	production
/atlas/analysis	analysis
/atlas/students	students

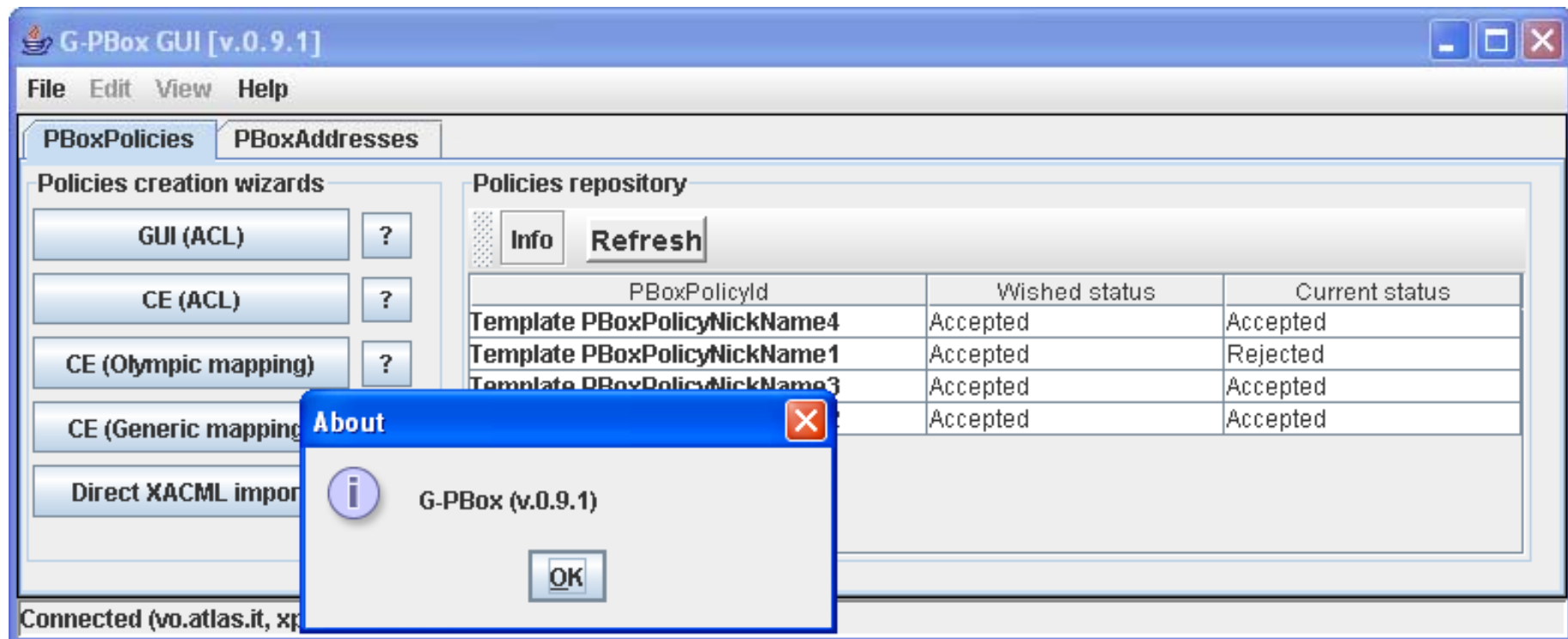
  

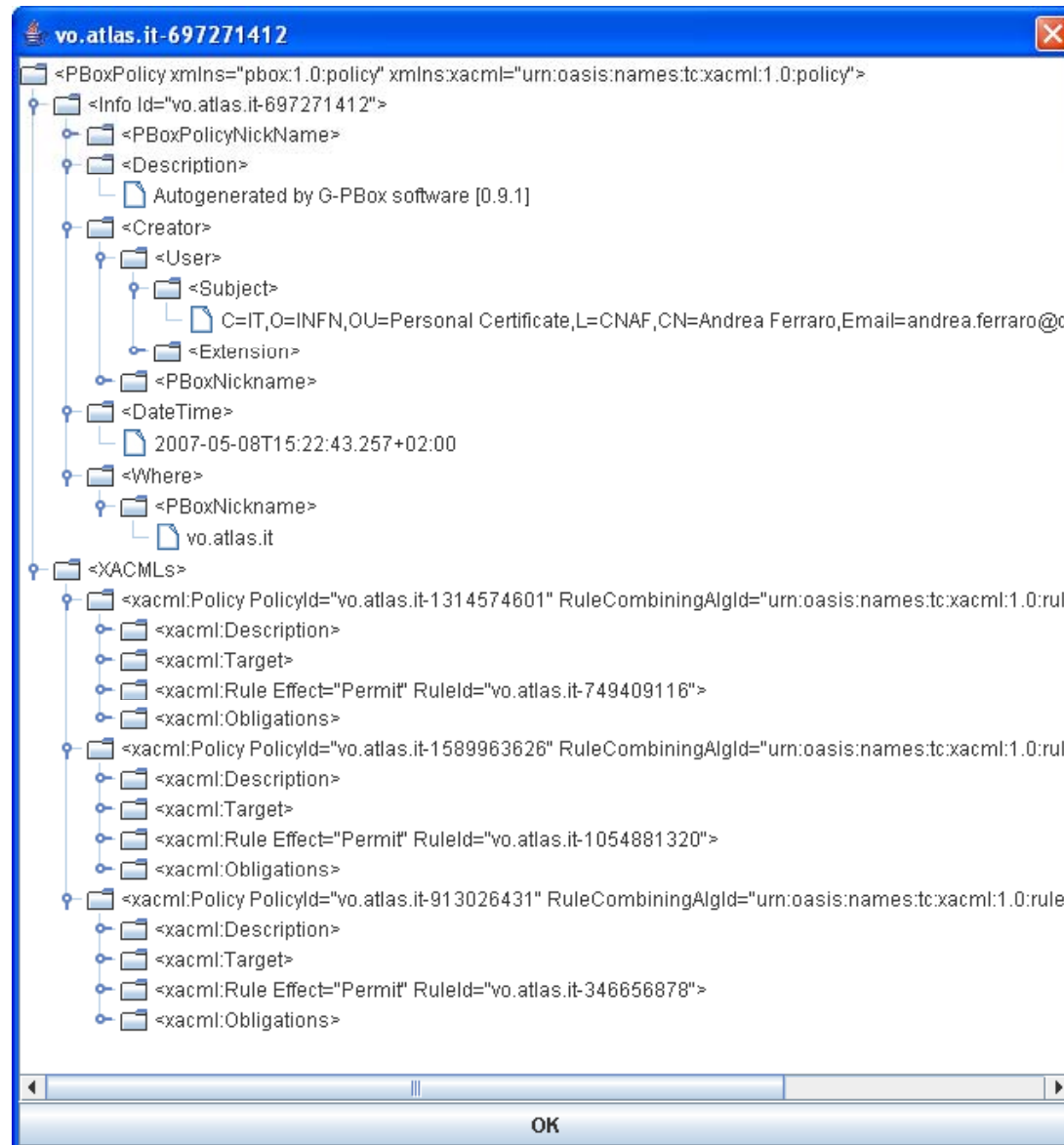
Site Policies (almost static)	
<b>ACBR</b>	<b>Unix ID</b>
production	atlas_high
analysis	atlas_mid
students	atlas_low



- **VO policies management**
  - If VO admins want to change relative priorities of different groups, all they need to do is change their policy in their VO, everything else is done by the system
- **Site independence and privacy**
  - Sites do not need to publish (ex BDII) the details of their internal setup
  - Sites are free to change their site-specific policies according to local constraints and rules







- **Vincenzo Ciaschini**
- **Andrea Ferraro**
- **Alberto Forti**
- **Antonia Ghiselli**
- **Alessandro Italiano**
- **Davide Salomoni**