



## **G-PBox Facts and status**

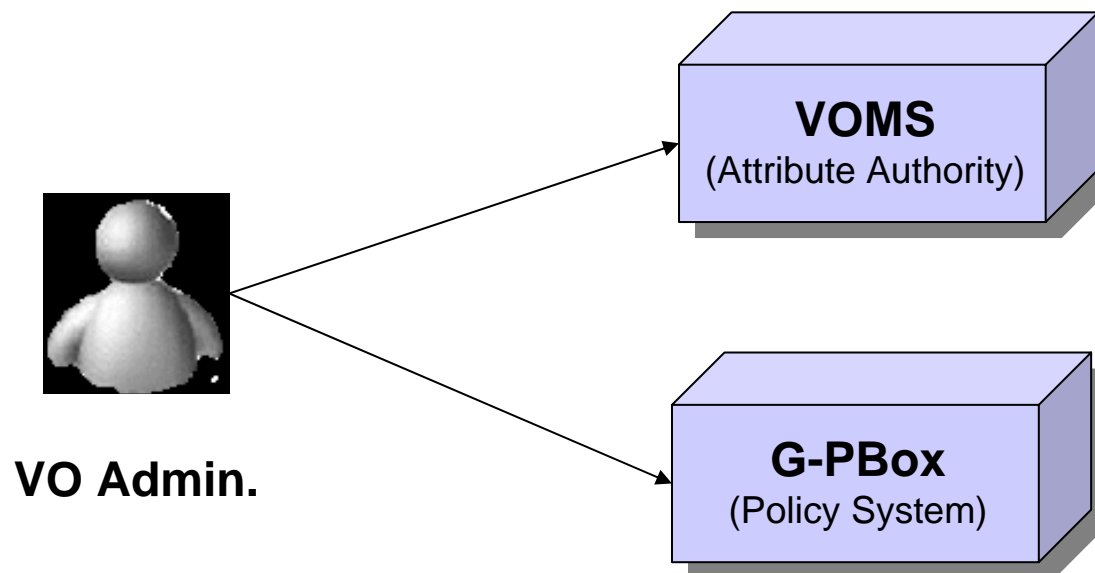
**Andrea Ferraro**

***JRA1 Authz Coord Meeting***

***January 18-19 2007***

***CNAF/INFN Bologna***

- *It is an highly distributed policy management and evaluation framework*
- *It is the natural complement of VOMS*
  - *VOMS issues attributes*
  - *G-PBox uses them for policy evaluation.*



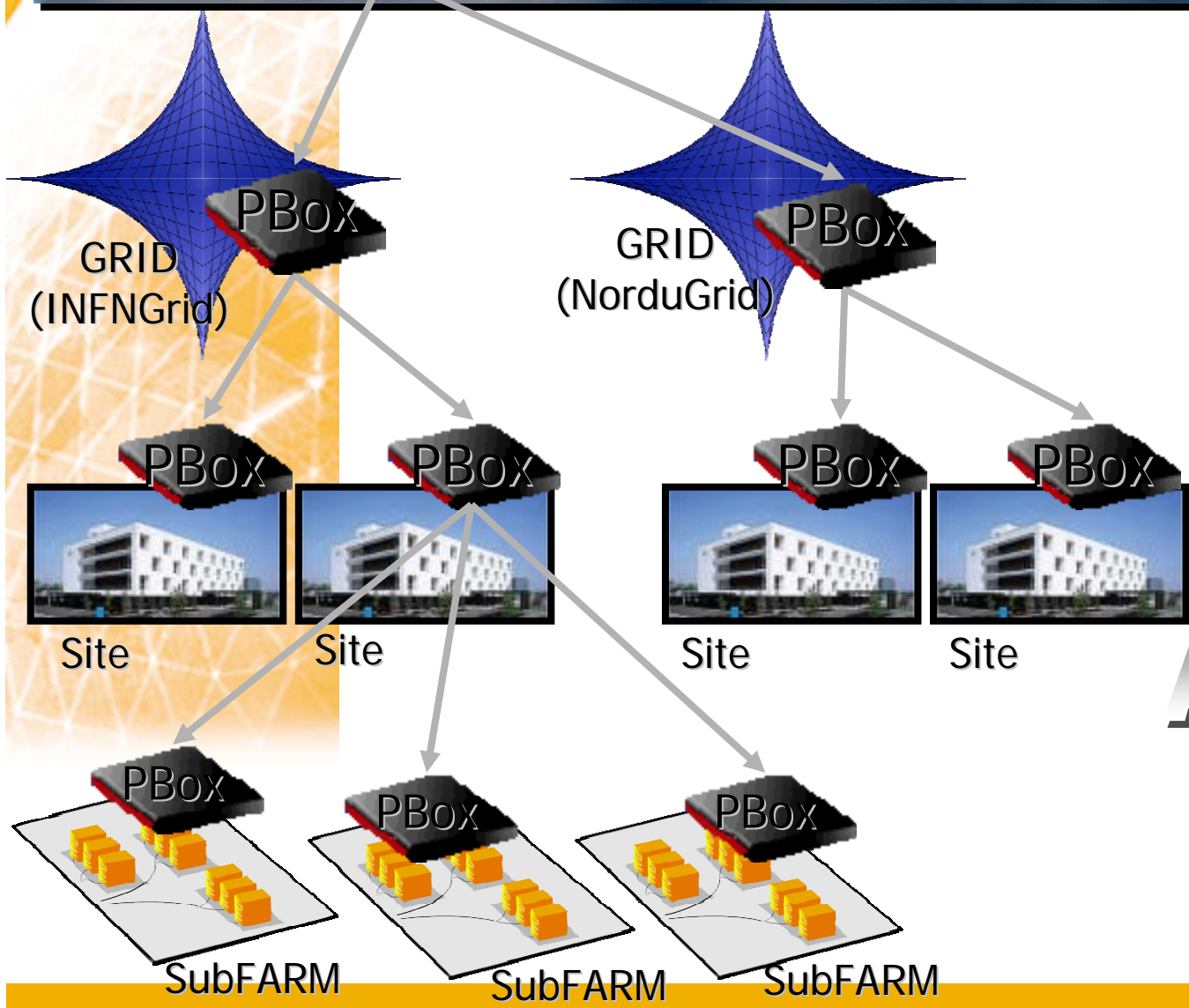
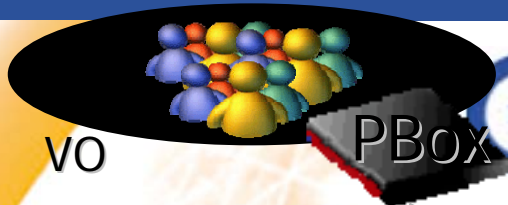


G-PBoxes are the basic elements of G-PBox

- They originate and distribute policies created by VO and Site admin
  - They evaluate requests from Resources/Services contacted by User
- One G-PBox (at least) for each VO (contacted by VO RBs)
  - One G-PBox for a Site or a brunch of Sites (contacted by Site CEs, SEs, etc.)

VO

Admins



SITE  
Admins



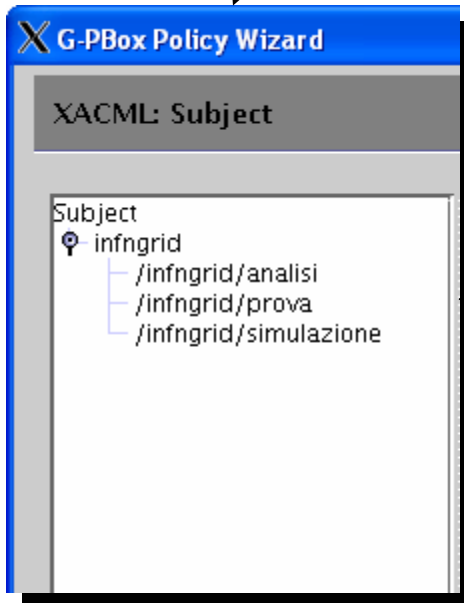
## G-PBox/VOMS relationship

- In the policy building phase (with the GUI)
  - During a policy creation (by a VO/Site admin) the VO G-PBox asks to the VO VOMS the VO groups/subgroups list
- In the policy evaluation phase
  - During a policy evaluation every G-PBox-compliant service/resource that is accessed by a Grid user need the VOMS user proxy extensions in order to evaluate the user credential to send to the G-PBox

What are the groups and subgroups of VO infngrid ?

G-PBox  
(VO=infngrid)

VOMS  
(VO=infngrid)

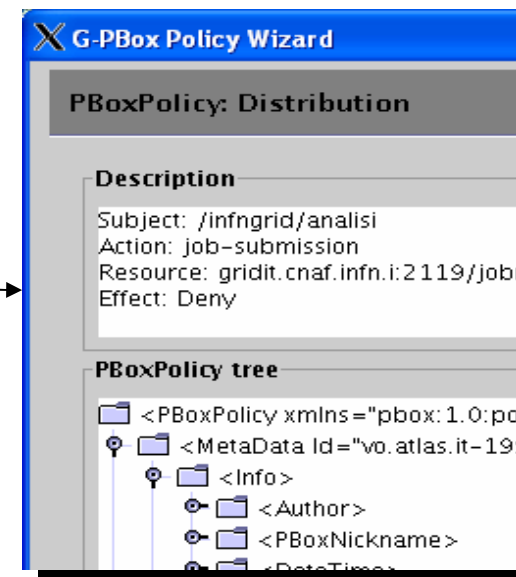


X G-PBox Policy Wizard

XACML: Subject

Subject

- infngrid
  - /infngrid/analisi
  - /infngrid/prova
  - /infngrid/simulazione



X G-PBox Policy Wizard

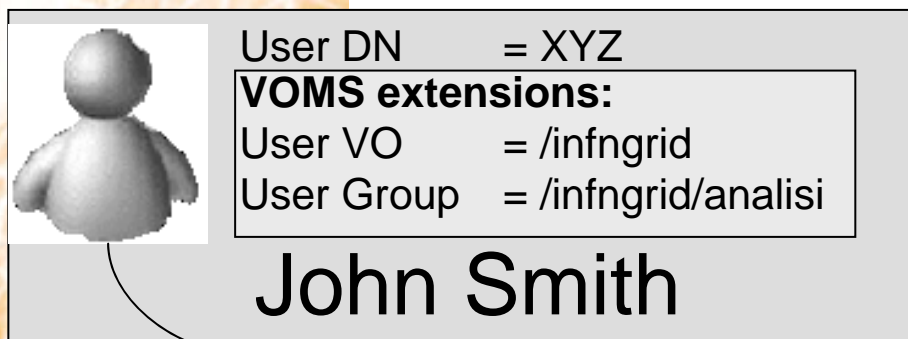
PBoxPolicy: Distribution

Description

Subject: /infngrid/analisi  
Action: job-submission  
Resource: gridit.cnaf.infn.i:2119/jobr  
Effect: Deny

PBoxPolicy tree

- <PBoxPolicy xmlns="pbox:1.0:po">
- <MetaData Id="vo.atlas.it-199">
- <Info>
- <Author>
- <PBoxNickname>
- <DateTimes>



User DN = XYZ  
**VOMS extensions:**  
User VO = /infngrid  
User Group = /infngrid/analisi

**John Smith**

Service/Resource X

G-PBox Plugin

Is there any policy for service/resource X about user John Smith ?

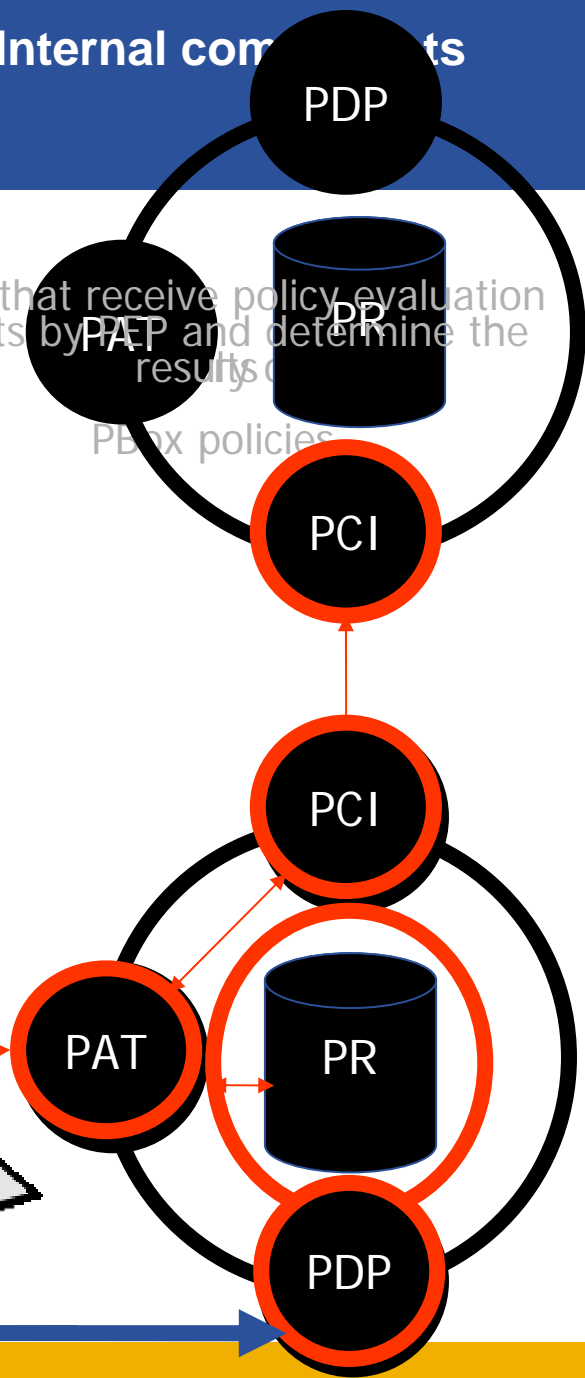


G-PBox

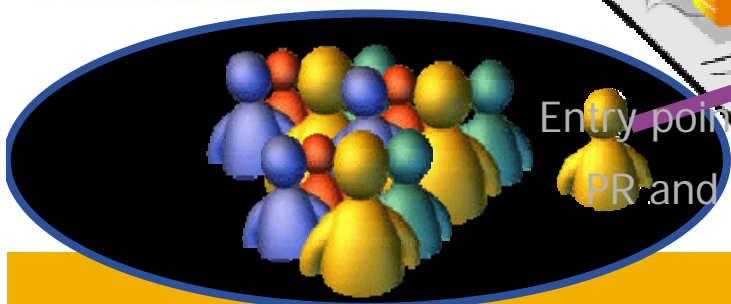
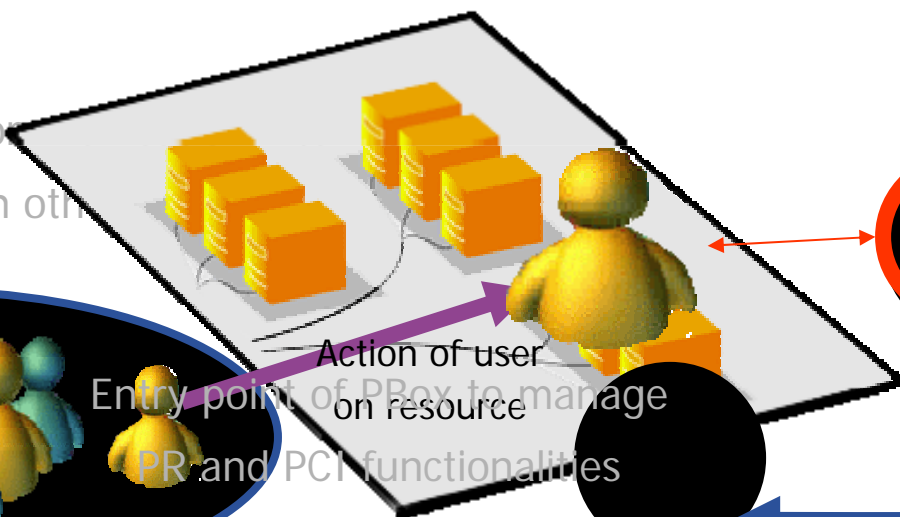
G-PBox response

- 1 internal component
- PR
- 3 boundary components
- PCI
  - PAT
  - PCI
  - PAT
  - PDP

Module that receive policy evaluation requests by PAT and determine the results of PBx policies



Co...  
with oth...



Entry point of PBx to manage PR and PCI functionalities



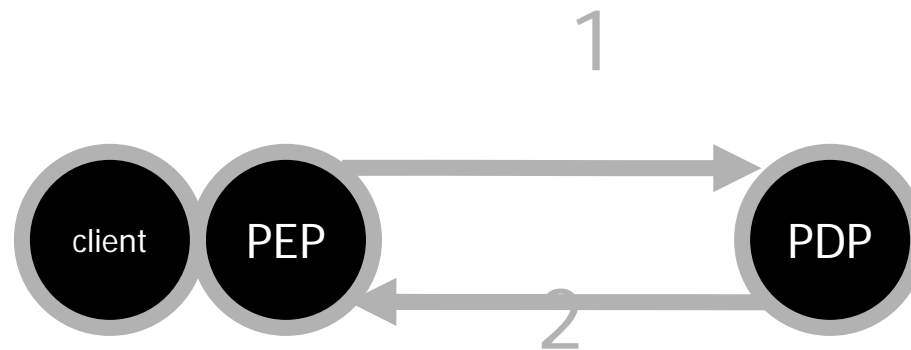


- **Policy propagation ensures that a PBox will always be capable of evaluate the last set of accepted policies even in case of network failures.**
  - Propagation only happens among neighboring levels on a direct father/child relationship.
  - Site admins will be able to explicitly:
    - Know the VO wishes, and check them against an existent AUP.
    - Grant or refuse them.

- **There are 2 kinds of policy status: Wished and Current.**
- **The first one is created by the owner of the policy and is the status the creator wants the policy to have.**
- **The second one is relevant only for myself. If I accept a policy coming from another level I have to change the current status from *unknown* to *accepted*, then I have to update my PDP server.**
  - It is possible to setup a PBox as a “slave” of another PBox if automatic acceptance is desired.
    - Example: sublevels of a site PBox.

A **client (LCMAPS or gJAF)** must implement a PEP (Policy Enforcement Point)

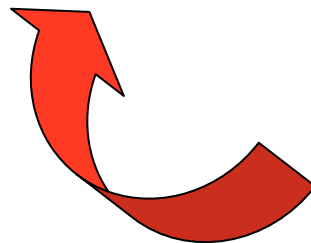
- The client sends a request to its PEP, which rewrites it into the correct syntax and sends it to the PDP of its PBox (1)
- The PDP of the PBox sends back its answer (2)
- The PEP translates the answer in a format recognized by the client.
- Only ONE request and answer for each evaluation.



– inter-VO resource sharing is in place

– intra-VO resource sharing is the new challenge

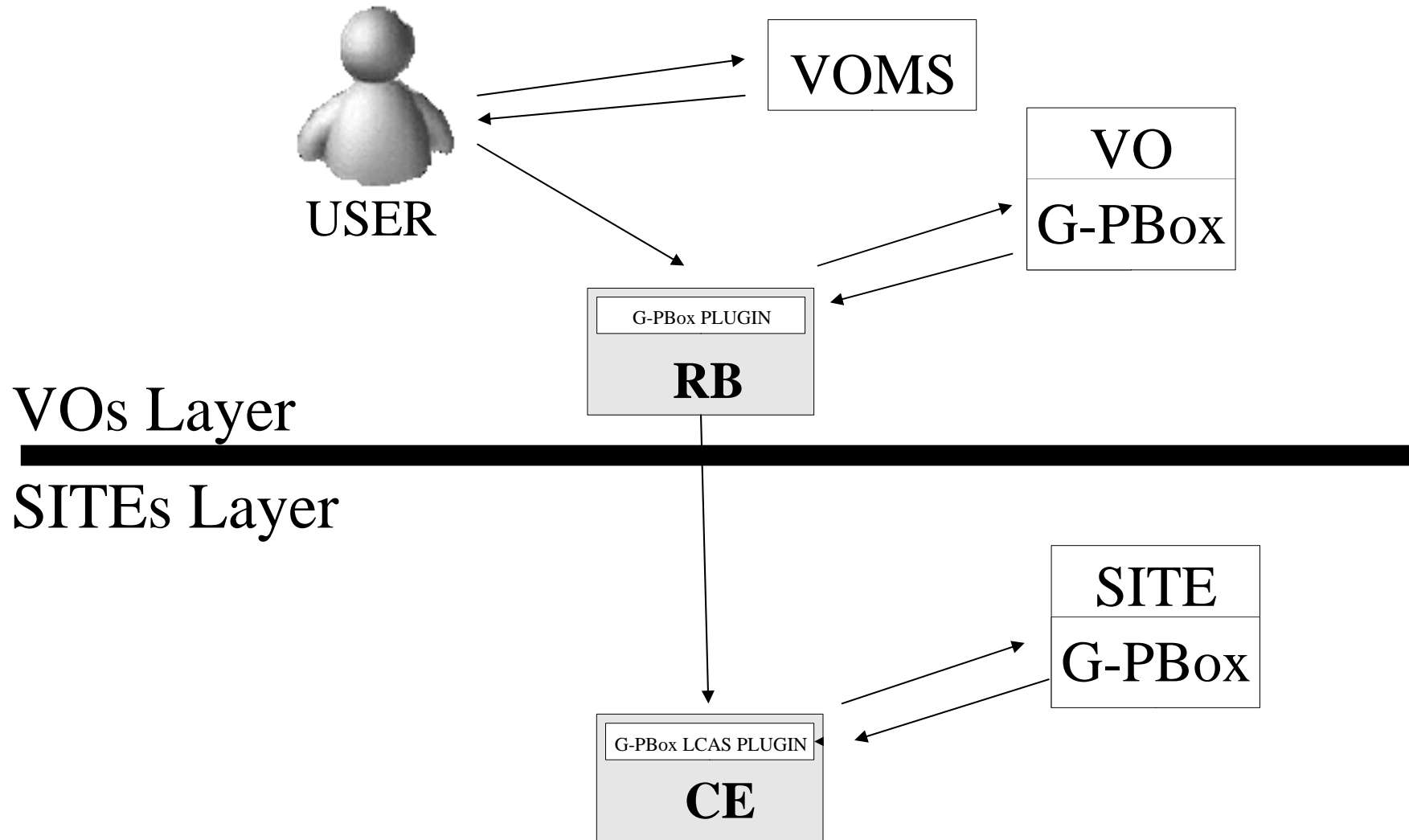
- Fair share: to set system utilization targets for VO internal groups/roles
- Priority: to set which job execute first among the queued ones



**WE WANT TO FACE  
THE CHALLENGE!!!**

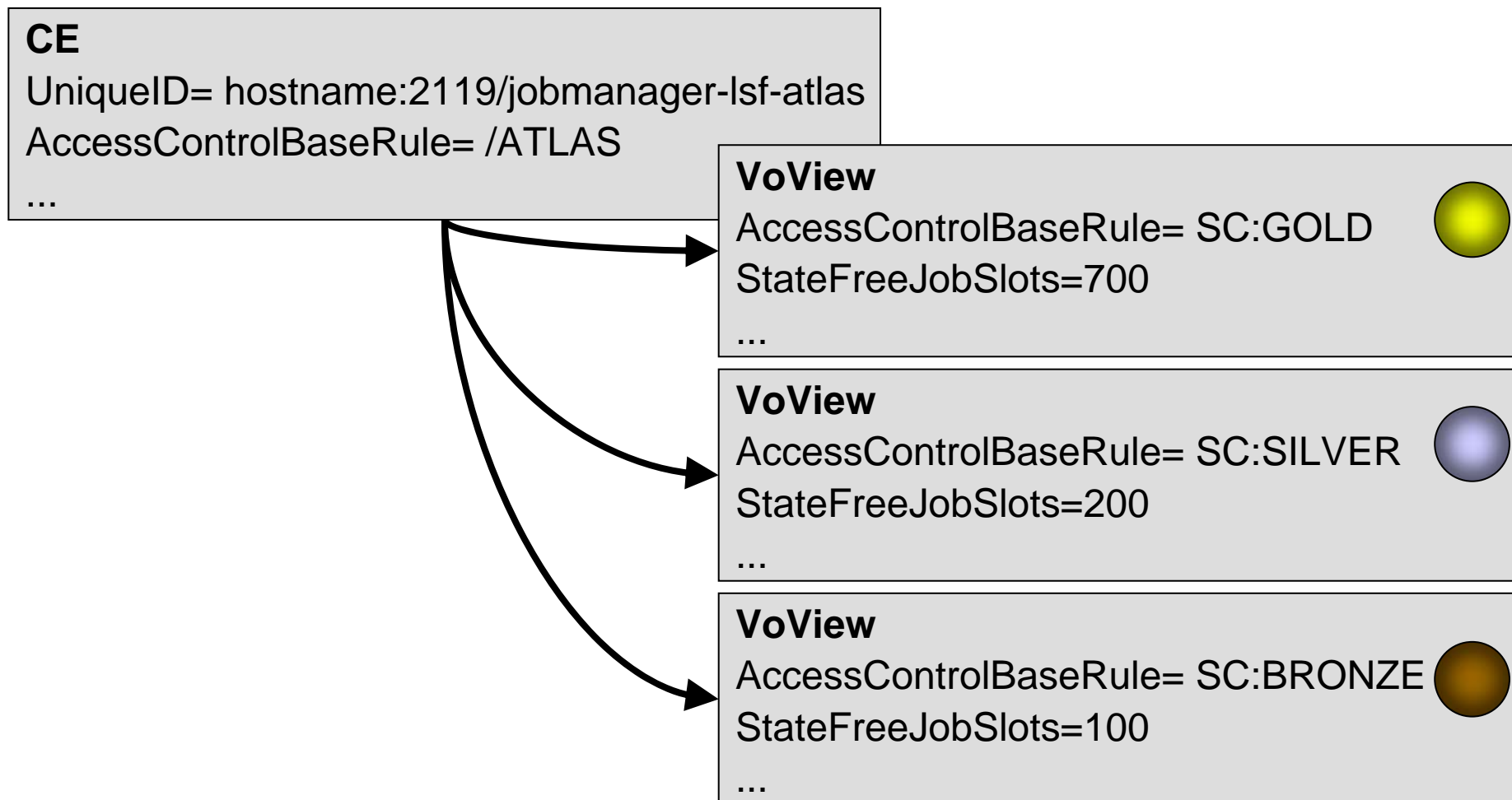
**(1) G-PBox system**

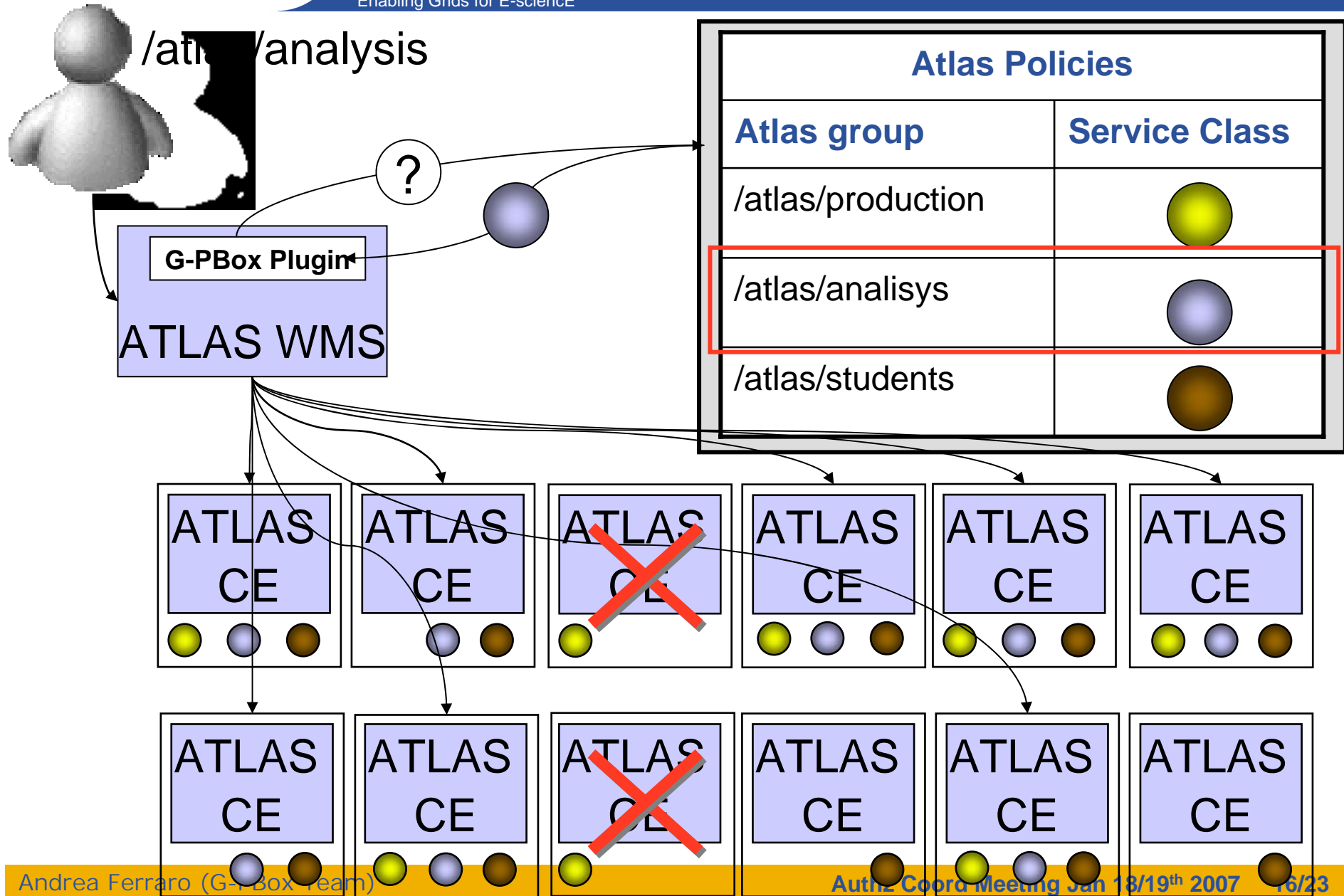
**(2) Services Classes for CEs**



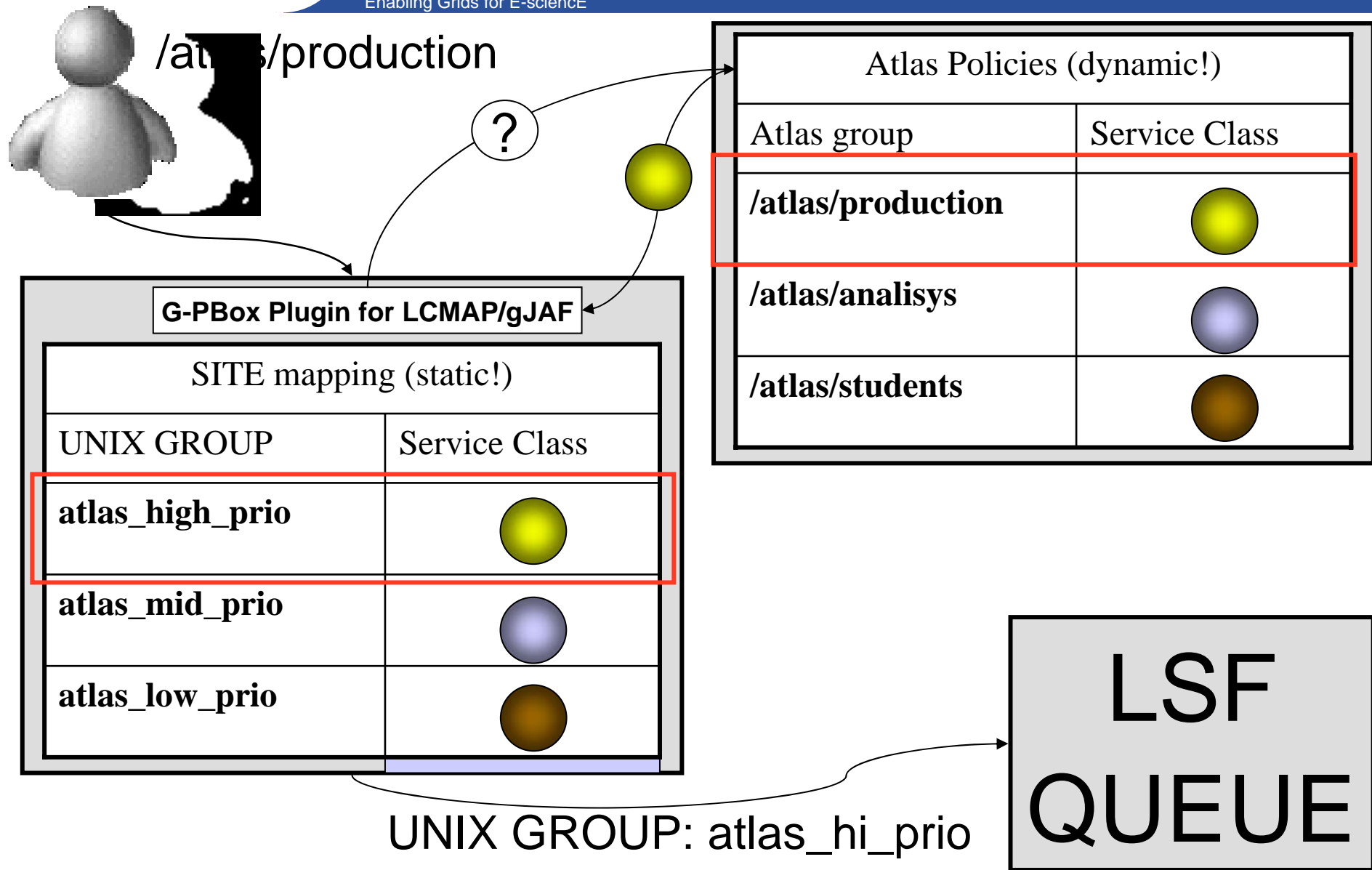
## (2) Services Classes for CEs

- A CE (queue) for each VO
- Each VOView maps to a service class (SC:GOLD, SC:SILVER, SC:BRONZE)









- **G-PBox server administration (develop stage):**
  - Start/stop/status
  - Remote diagnostic
- **G-PBox policies administration:**
  - Policy Repository management
  - Policy editor (very simple)
  - Policy structure view (PBoxPolicy metadata and XACML)
  - Current Policy Status management
  - Wished Policy Status management

- **Policies are expressed in XACML 1.0**
  - XACML can be extended to also support policies needing external data (ex: monitoring and accounting)
    - It is done on a (very) limited set.
    - Will be generalized to generic attributes.
    - Allows the implementation of policies requiring knowledge of the current grid status. E.g: “User X is allowed to submit a job only if the current disk usage of group /atlas/phys is less than 1T”
  - The mechanism of Obligations is used to support administration policies.

- **We have a prototype !**
  - Committed to the gLite CVS
  - Provides the basic described features
  - Tested by:
    - LHCb
    - EGEE preview team (D.Cesini)

- **With the prototype:**
  - ACL policies
  - Local policies (user mapping)
  - Simple RBAC policies:
    - Depending on just one VOMS group/role.
  - Static Policies (quota, cpu share, etc... if they are specified by the policy and/or the PEP)
    - Need much support for this on the services though. Enforcement and data collection.
  
- **With the final product (when integration with accounting and monitoring is complete):**
  - Fair share.
  - Generic Storage.
  - Complex RBAC Policies
    - Depending on a combination of VOMS group/roles.
  - Policies in which the data needed for evaluation is taken from the environment.
    - Much less support needed from services. Essentially enforcement only.

- **APIs for C/C++/Java are available.**
  - Services can use them to automatically construct XACML requests, send them and parse XACML responses.
    - Not only Deny/Allow are returned, but also Obligations
  - However, services must have knowledge of possible obligations and honor them
  - Services must do the real enforcements based on G-PBox answers.
- **Demo quality implementations are available for LCAS, LCMAPS and RB**
- **gJAF integration is welcome!!!**

- **Vincenzo Ciaschini (INFN/CNAF)**
- **Andrea Ferraro (INFN/CNAF)**
- **Marco Cecchi (INFN/CNAF)**
- **Alberto Forti (INFN/CNAF)**