G-PBox and Policies

Alberto Forti
19/06/2007

www.eu-egee.org

Information Society and Media

Summary

- Problem statement
- G-PBox
- G-PBox status
- The Job Priority use case
  - what's going on
  - a G-PBox solution
- Tests
- Roadmap
- Conclusions

Problem statement

- AuthN/AuthZ management on the grid is rapidly changing and evolving
  - VOs continuously add/modify/remove users, groups and roles all the time
  - VOs require different execution priorities for different users
  - VOs require dedicated resources for specific users in delicate periods (see DataChallenges, etc.)
  - funding agencies can force constraints affecting resource allocations
  - sites may want to enforce site-specific policies

Our approach: VOMS + G-PBox

- VOMS is an Attribute Authority
  - it issues attributes for users (roles, groups, etc.)
- G-PBox is a Policy System
  - it allows VO and Site admins to write policies for resources/services
  - it uses VOMS attributes

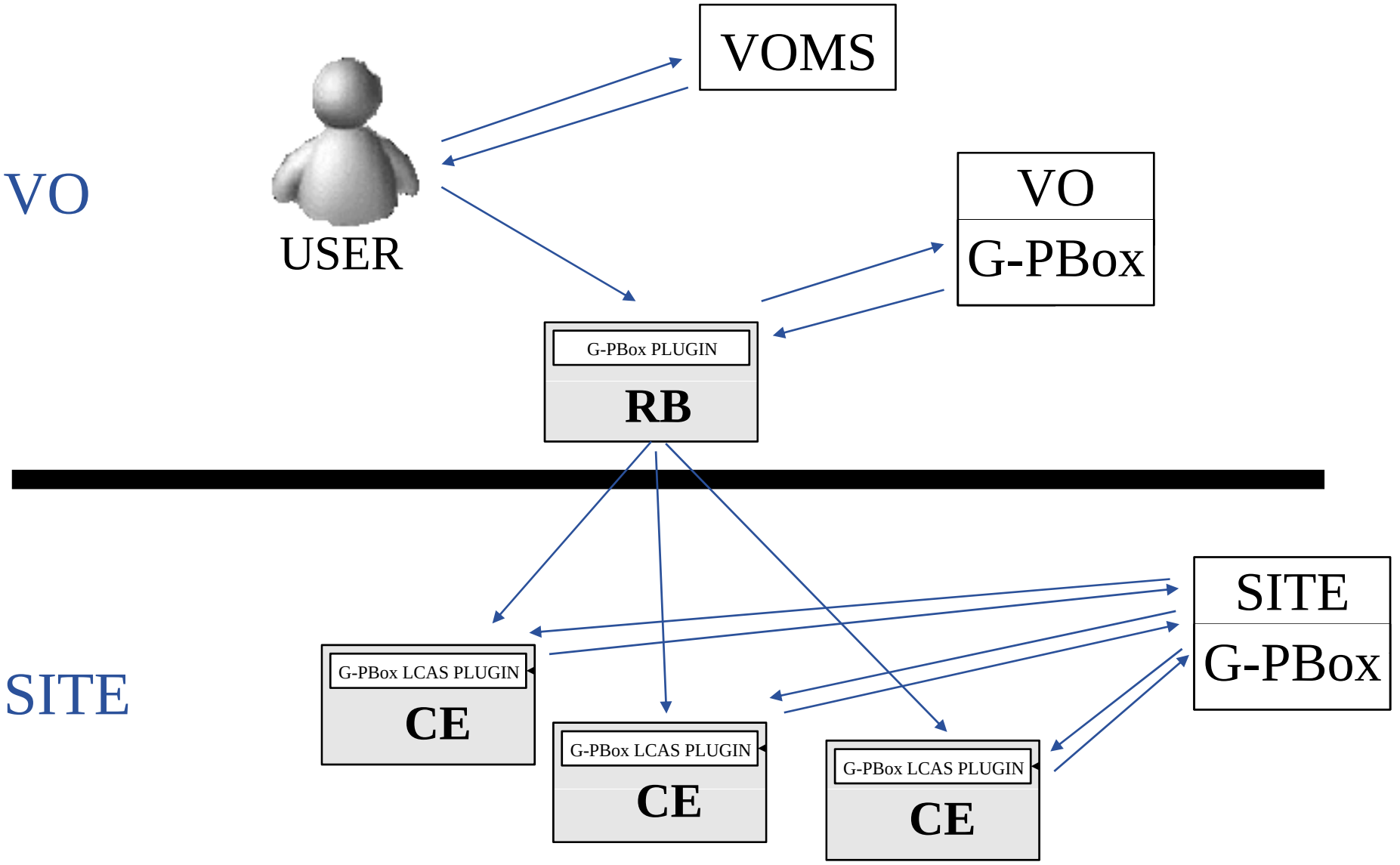
G-PBox

- It provides a robust and decentralized way to distribute policies between VOs and Sites
- It is an elegant approach that improves the relationship between VOs and sites
  - VOs and Sites share contracts (XACML policies) to regulate resource usage
- It is queried by:
  - services (as a VO WMS)
  - resources (as CEs and SEs) also not owned by VOs

G-PBox (2)

- VO G-PBox is managed by VO administrators
  - to write policies for internal VO groups/roles (defined in the VO VOMS server)
  - to manage policies received from Site G-PBoxes
- Site G-PBox is managed by site administrators
  - to write policies for internal sites users
  - to manage policies received from VO G-PBoxes

VOMS/G-PBox


VOMS
VO
USER
VO
G-PBox
G-PBox PLUGIN
RB
SITE
SITE
G-PBox
G-PBox LCAS PLUGIN
CE
G-PBox LCAS PLUGIN
CE
G-PBox LCAS PLUGIN
CE

G-PBox status

- It has been completely re-engineered in the last months
- GUI
  - definition of more complex XACML policies
  - integration with VOMS servers to retrieve role/groups
  - improvement of the policy management facility
- Server
  - refactoring of packages during Etics transition
  - adopted org.glite.security facilities
    - GUI <->G-PBox and G-PBox <-> G-PBox
  - XIndice DB to eXist DB transition
  - improved the internal policy structure management

Job Priority

- User gets a VOMS proxy with some group/role
  - i.e. /atlas/Role=production
- WMS forwards user jobs to the CE considers the VOViews matching the VOMS FQAN for the matchmaking
  - VOViews provide a way for publicizing the relevant characteristics of a CE on a FQAN-based way
- CE translates the user FQAN into a local user depending on a LCMAPS configuration file
- LRMS is configured to grant different priorities/shares to different users/groups

Job Priority (Problem)

- CEUniqueID: ce01.ific.uv.es
  1. GlueVOViewLocalID: atlas
     - GlueCEAccessControlBaseRule: VO:atlas
     - GlueCEStateWaitingJobs: 0
  2. GlueVOViewLocalID: /atlas/Role=production
     - GlueCEAccessControlBaseRule: VOMS:/atlas/Role=production
     - GlueCEStateWaitingJobs: 1000

- *PROBLEM (considering a rank based on waiting jobs):*
  - *User with FQAN:/atlas/Role=production matches both (1) and (2)*
  - *the best match is (1)*
  - *LCMAPS will map the FQAN to the user associated with VOMS:/atlas/Role=production (2)*

Job Priority (short term solution)

- Make the VOViews mutually exclusive
- CEUniqueID: ce01.ific.uv.es
  1. GlueVOViewLocalID: atlas
     - GlueCEAccessControlBaseRule: DENY:/atlas/Role=production
     - GlueCEAccessControlBaseRule: DENY:/atlas/Role=software-mgr
     - GlueCEAccessControlBaseRule: VO:atlas
     - GlueCEStateWaitingJobs: 0
  2. GlueVOViewLocalID: /atlas/Role=production
     - GlueCEAccessControlBaseRule: VOMS:/atlas/Role=production
     - GlueCEStateWaitingJobs: 1000

Job Priority (short term solution)

- This solution does not scale:
  - including new groups and roles will be quite some work and involves all sites
  - changing shares between different groups/roles of the same VO does not seem trivial either
- The information system is not the right place for authorization statements

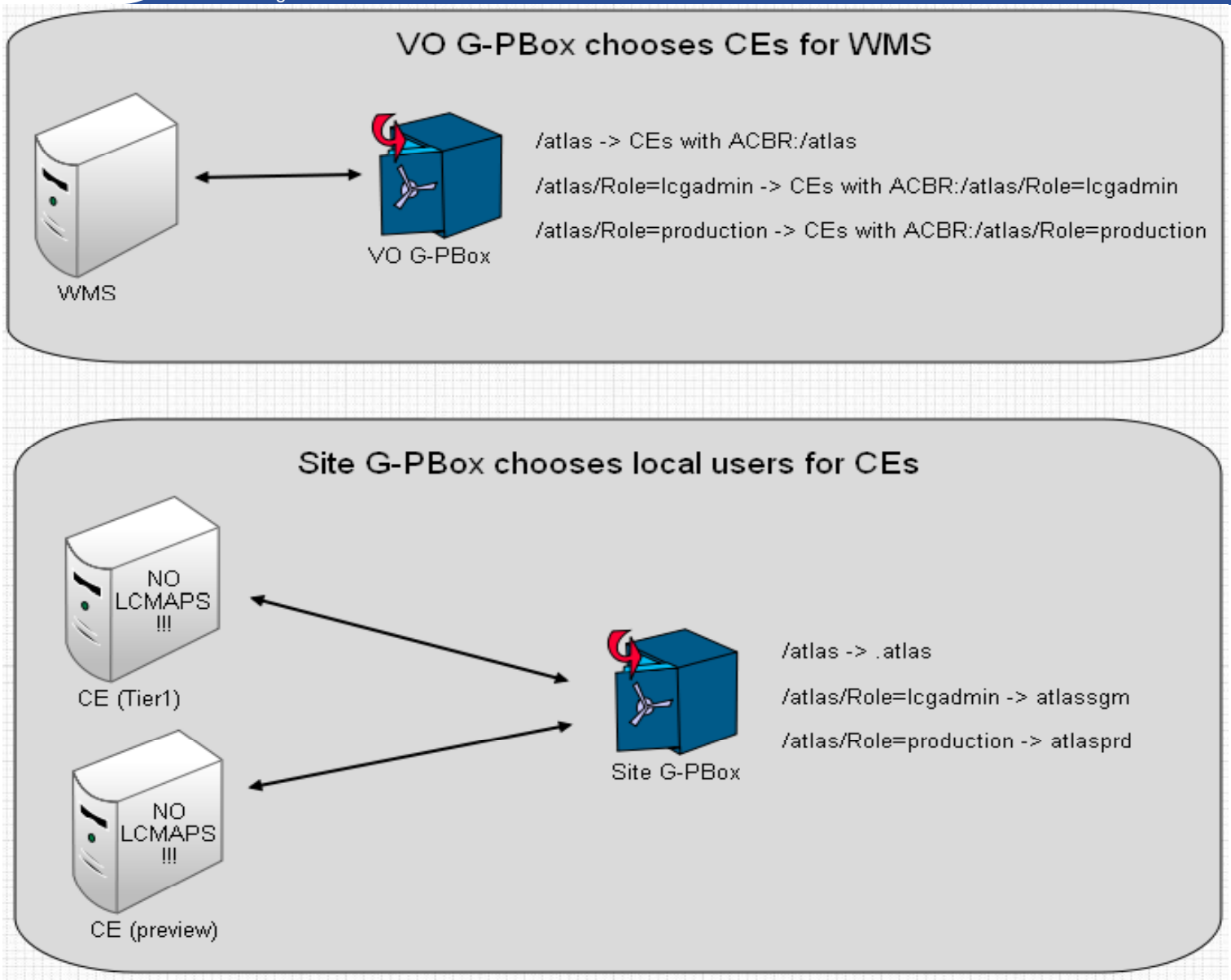
Job Priority (G-PBox solution)

- Agreement between VO admins and site admins on VO shares names
- VO administrator
  - writes two policies:
    - Policy (for WMS): `FQAN: /atlas/Role=production` → `ACBR:VOMS:/atlas/Role=production`
    - Policy (SHARE POLICY for CEs): `FQAN:/atlas/Role=production` → `Share: high`
- Site administrator
  - writes one policy (and accepts/reject SHARE POLICY)
    - Policy (SHARE POLICY for CEs): `FQAN:/atlas/Role=production` → `Share: high`
    - Policy (for CEs): `Share: high` → `User: atlasprd`

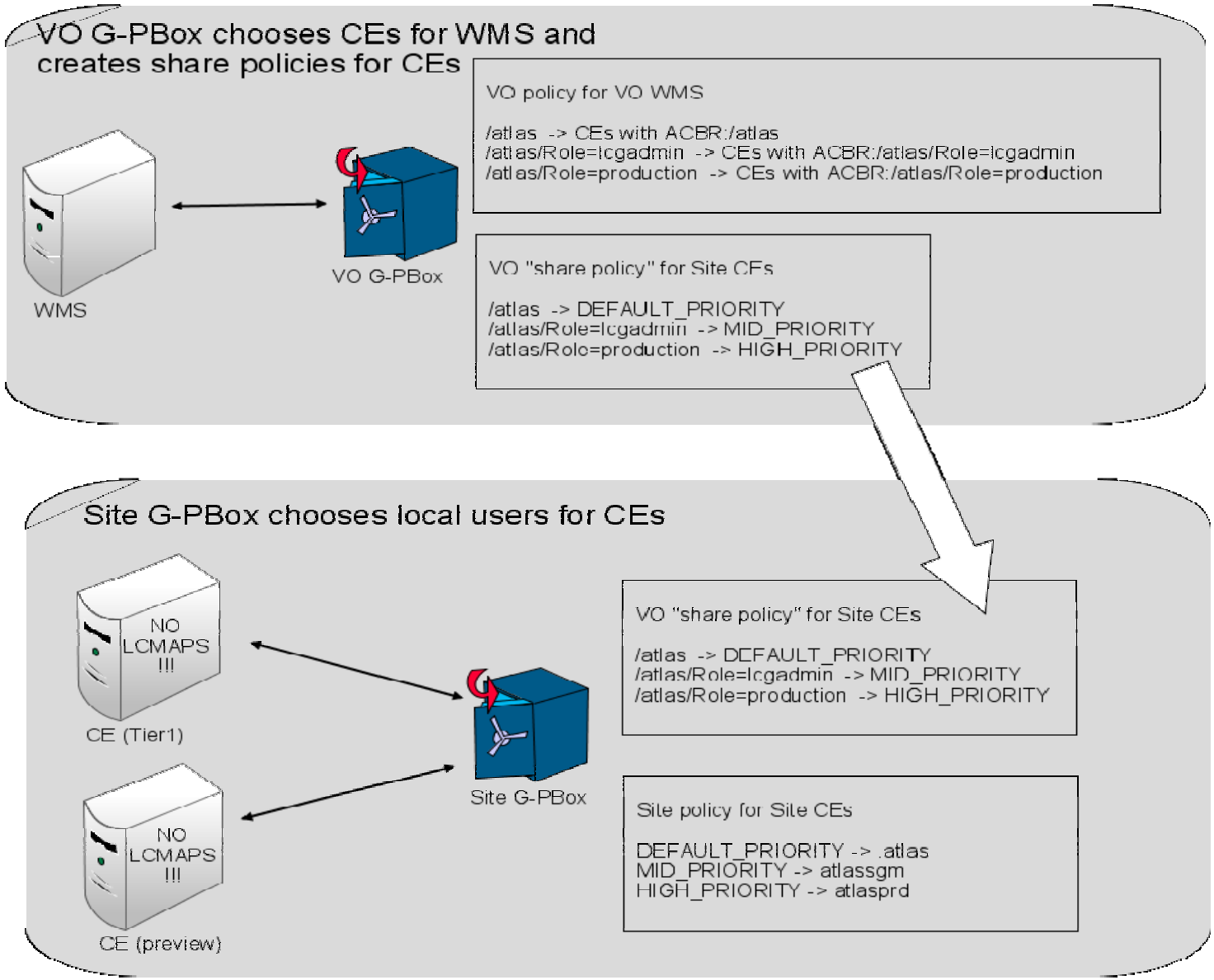
Job Priority (G-PBox solution)

- Very easy to include/remove groups and roles
- Very easy to change shares between different groups/roles of the same VO (SHARE POLICIES)
- Sites can accept or reject SHARE POLICIES
- Sites are not obliged to change published BDII infos every time VOs change their user/groups priority strategy

Ongoing tests (in preview TB)



Next tests (in preview TB)



First tests results

- Functionality
  - Site G-PBox: OK (internal tests), OK (preview TB)
  - VO G-PBox: OK (internal tests), ongoing (preview TB)
  - dynamic policy modifications: OK (internal tests), immediately after the VO G-PBox tests (preview TB)
- Performance
  - Site G-PBox (with 3500 policies):
    - 1000 Globus-job-run
      - *CE with G-PBox: mean execution time 6.453s (error 0.007)*
      - *CE without G-PBox: mean execution time 6,522s (error 0.003)*
  - VO-G-PBox:
    - Ongoing
- Test results:
  - https://twiki.cnaf.infn.it/cgi-bin/twiki/view/GPBox/WebTests

Roadmap

- From June 1, ’07 to July 20, ‘07:
  - performing of short term and long term preview tests
  - bug fixing and code improvement
  - consolidating Etics porting
  - packaging (RPMs, Release Notes, etc.)
- From July 23, ’07:
  - Release of G-PBox 1.0
  - Tests open to VOs and Sites

Conclusions

- G-PBox is a flexible solution for authorization issues in Grid
- G-PBox is currently supported by gLite-WMS and lcg-CE (lcmpas_gpbox plugin)
- G-PBox will be supported as an external PDP by gLite gJAF (used by CREAM CE)
- G-Box adoption is not invasive:
  - a CE is not required to use G-Box if there is a VO G-PBox
  - CEs can use G-PBox without requiring a VO G-PBox
- Considering Job Priority issues:
  - share becomes easy to change (no BDII changes for modify shares)
  - BDII continues to be an information system and do not used also as an authorization trick
- The same G-PBox can be used to manage many authorization contexts (e.g. Job Submission, Data access on SEs, etc.)