

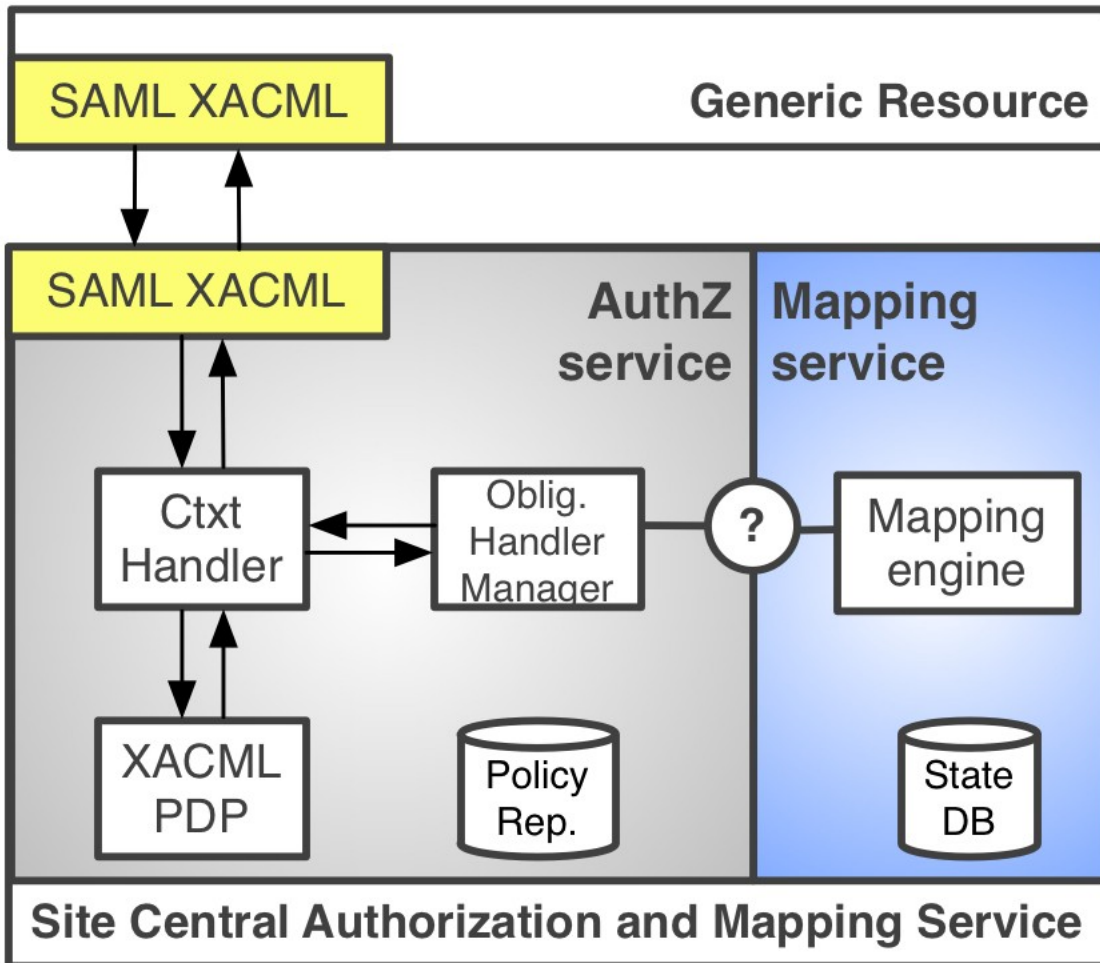
# G-PBox: current role and future development

*Alberto Forti*

*Middleware Security Group Meeting*

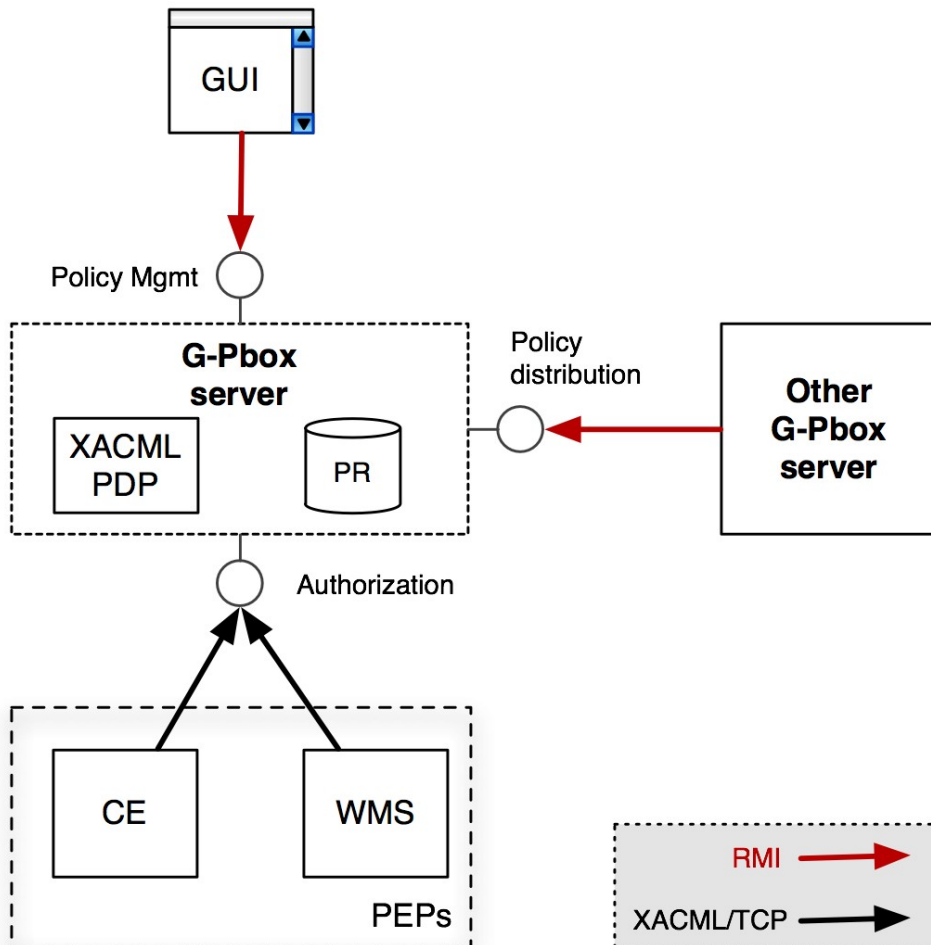
*December 6-7, 2007. Berkeley.*

- **Authorization and Mapping**
- **Proof of concept prototype**
- **G-PBox GUI overview**
- **Future plans**

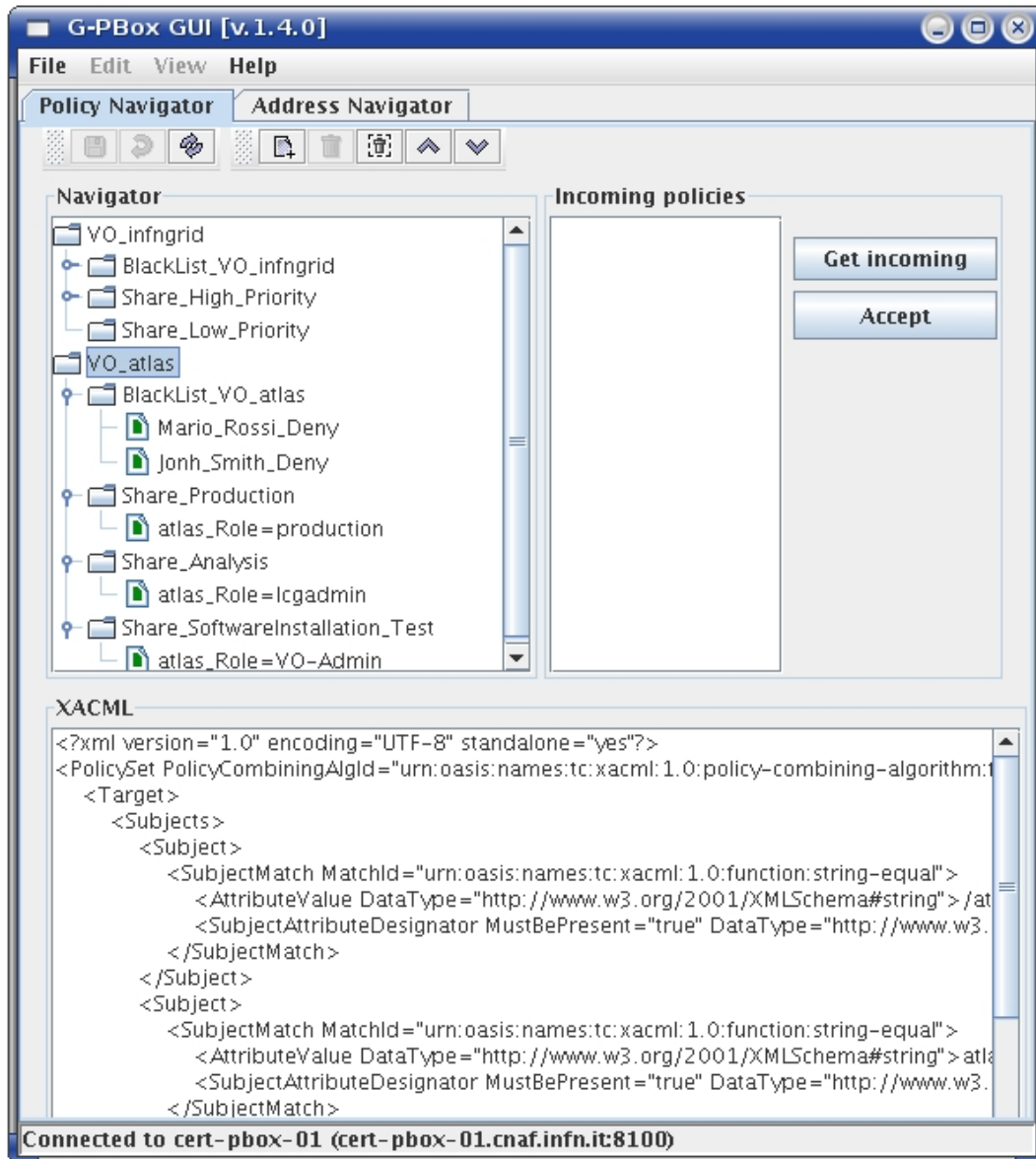


- Presented at the EGEE AH meeting based on Yuri's draft design proposal
- Modular architecture that integrates authorization and mapping with clear task separation
- Allows for integration of the mapping function with a XACML PDP

- **Implemented prototype**
  - Fully integrated with the G-PBox PDP
  - Preliminary implementation of the obligation handling mechanism
    - “fake” mapping engine
      - *shall we agree on the interface?*
- **Tested against gJAF that uses OpenSAML and GT clients**
  - Interoperable with the OpenSAML SAML-XACML extension implemented by Håkon Sagehaug
  - Two minor issues with GT clients:
    - the subject-id DN format
    - missing namespace in the XACML request
- **Advantages**
  - Fulfill the interface contract
    - a **real** XACML PDP behind the SAML-XACML interface
  - Flexible authorization management: not tied to the mapping service
    - Other services (e.g. WMS) could use the same authz policies (no mapping needed)
    - Straightforward policy distribution



- **Policy Administration Point (PAP)**
  - Policy Repository (Exist XML DB)
  - Administrative interface (Java swing GUI)
  - Policy distribution
- **Policy Decision Point (PDP)**
  - Customized Sun XACML engine
    - XACML v. 2.0 supported
  - Policies are kept in memory (snapshot of the PR)
- **Policy Enforcement Point (PEP)**
  - LCAS/LCMAPS plugin
  - WMS
  - Java, C/C++ APIs



**Navigator**

- VO\_infngriid
  - BlackList\_VO\_infngriid
  - Share\_High\_Priority
  - Share\_Low\_Priority
- VO\_atlas
  - BlackList\_VO\_atlas
    - Mario\_Rossi\_Deny
    - Jonh\_Smith\_Deny
  - Share\_Production
    - atlas\_Role=production
  - Share\_Analysis
    - atlas\_Role=lcgadmin
  - Share\_SoftwareInstallation\_Test
    - atlas\_Role=VO-Admin

**Incoming policies**


Get incoming

Accept

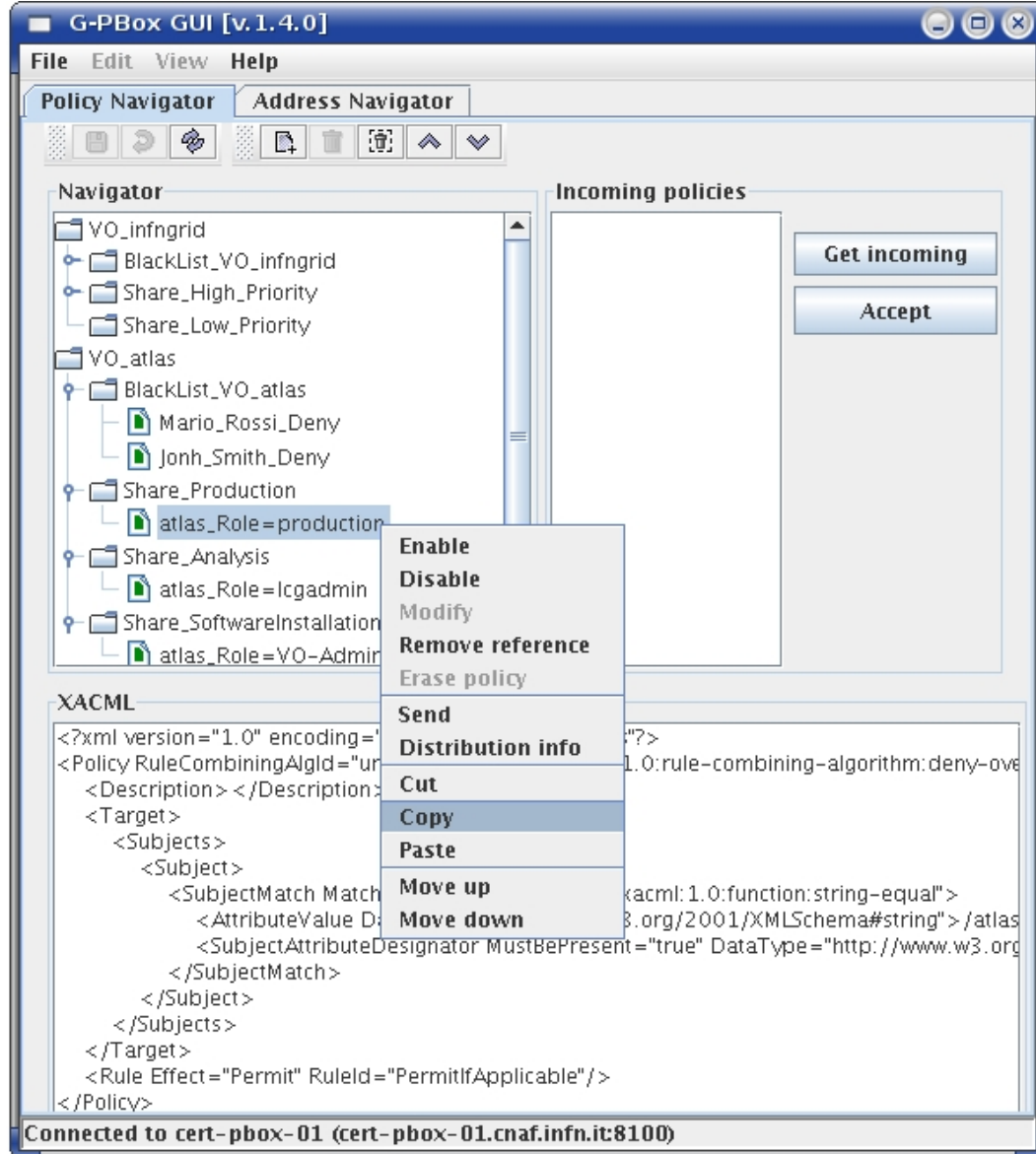
**XACML**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/at
          <SubjectAttributeDesignator MustBePresent="true" DataType="http://www.w3.
        </SubjectMatch>
      </Subject>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">atle
          <SubjectAttributeDesignator MustBePresent="true" DataType="http://www.w3.
```

Connected to cert-pbox-01 (cert-pbox-01.cnaf.infn.it:8100)

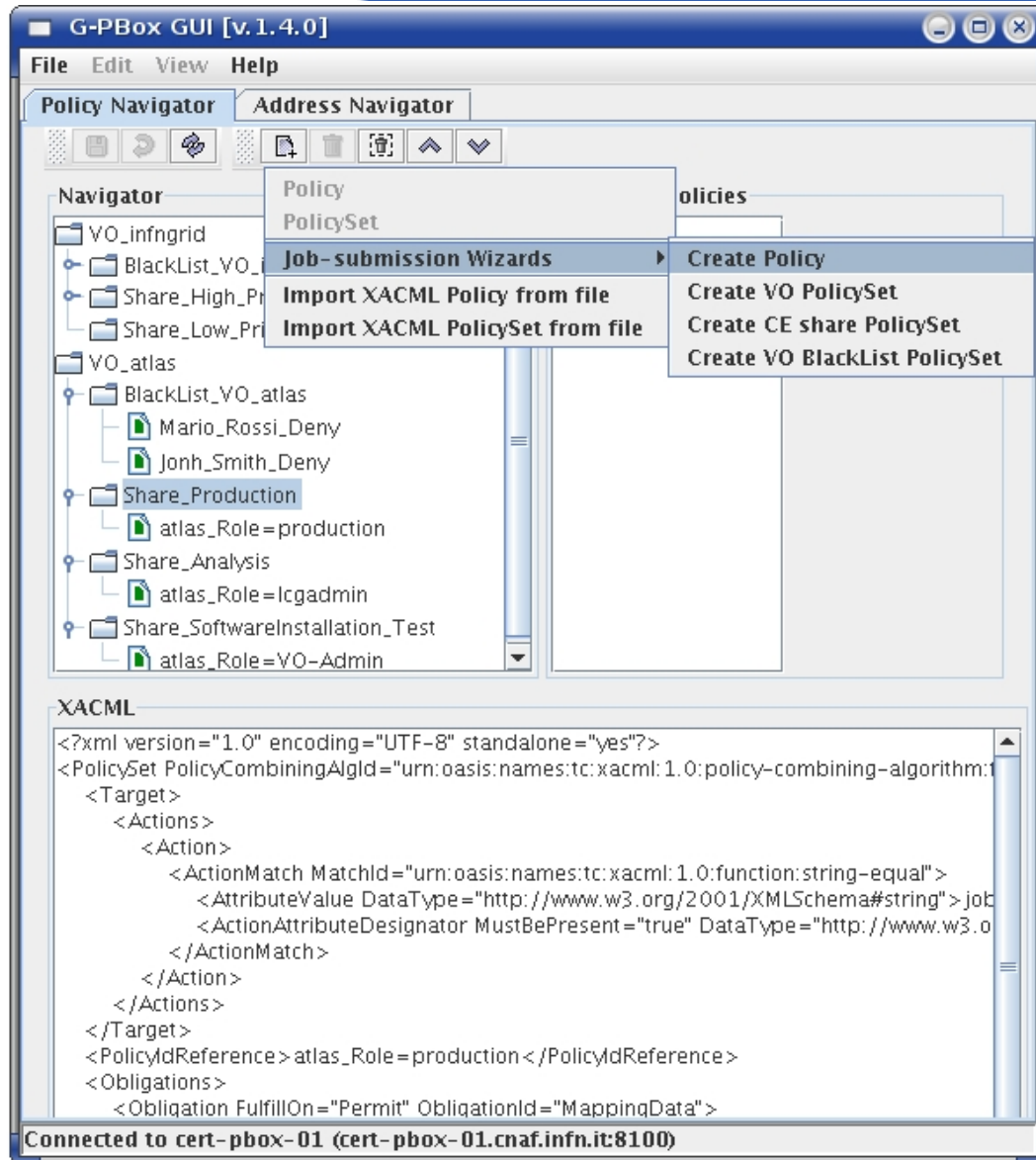
- Navigator
  - Policy Database snapshot
  - Refresh button  : synchronize the Policy DB with the PDP
- Incoming policies
  - Policies sent by other G-PBoxes
- XACML
  - XACML view of policies and policy sets

- **VO PolicySet: *VO\_infngrid, VO\_atlas***
  - Policy set containing policies of a specific VO
- **Share PolicySet: *Share\_High\_Priority, Share\_Production, etc.***
  - Policy set associated to a local user (or poolname)
    - If the matching policy is contained in a Share PolicySet, then the corresponding user (or poolname) is returned as an obligation
- **BlackList PolicySet: *BlackList\_VO\_infngrid, etc.***
  - Contains “Deny” policies used to ban users
- **Policies: *John\_Smith\_Deny, atlas\_Role=production, etc.***
  - To map users/groups/roles to a local user (for the batch system) insert the policy in the corresponding Share PolicySet
  - To change the mapping for a user/group/role move the policy to another Share PolicySet

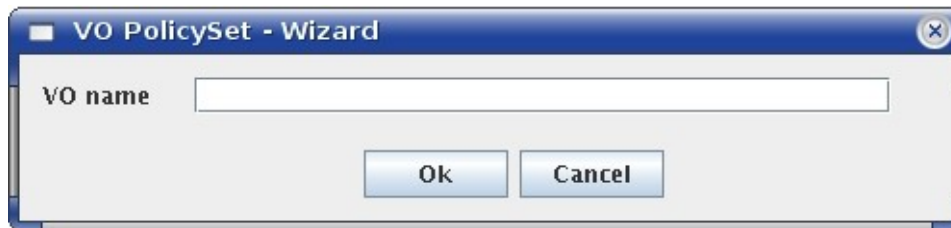


- Right mouse button popup menu for Policy/PolicySet
  - Basic management operations
    - Enable/Disable
    - Cut&Paste
    - Change order
  - Send policies to other G-PBoxes
  - Distribution info



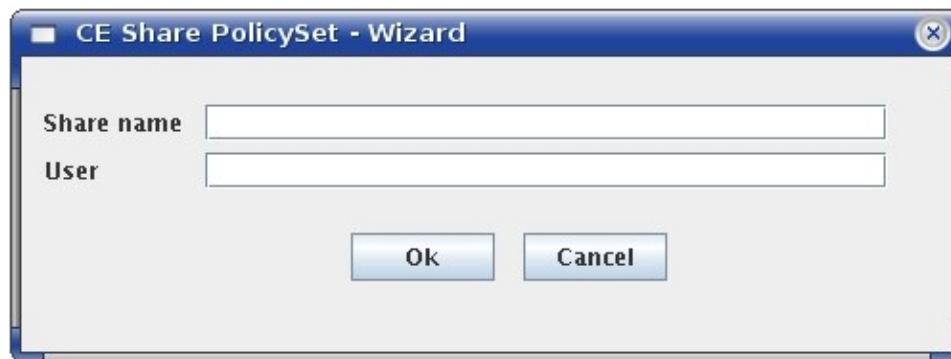


- **New Policy/PolicySet button**
  - Generic XACML editor
  - Wizards
    - Create Policy
    - VO PolicySet
    - Share PolicySet
    - BlackList PolicySet
  - Import XACML Policy/PolicySet from file



- **VO PolicySet**

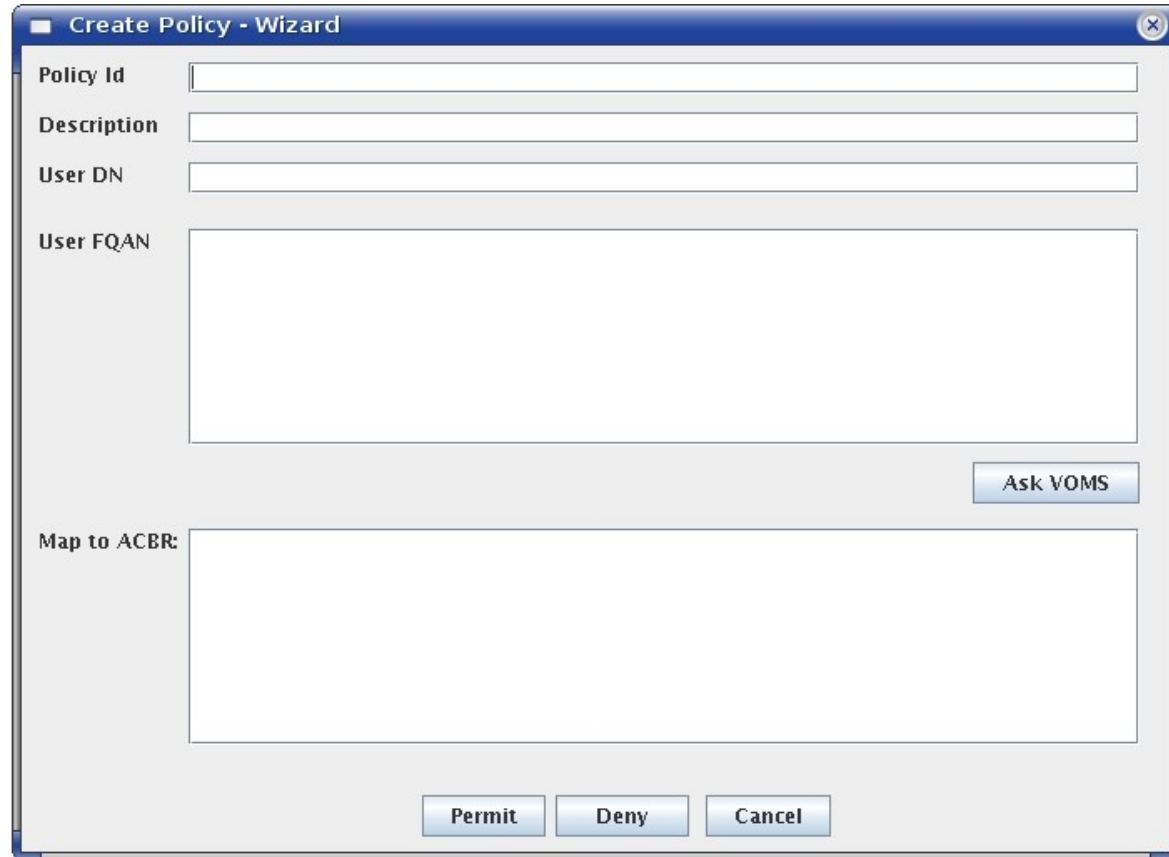
- Used to separate policies of different VOs



- **Share PolicySet**

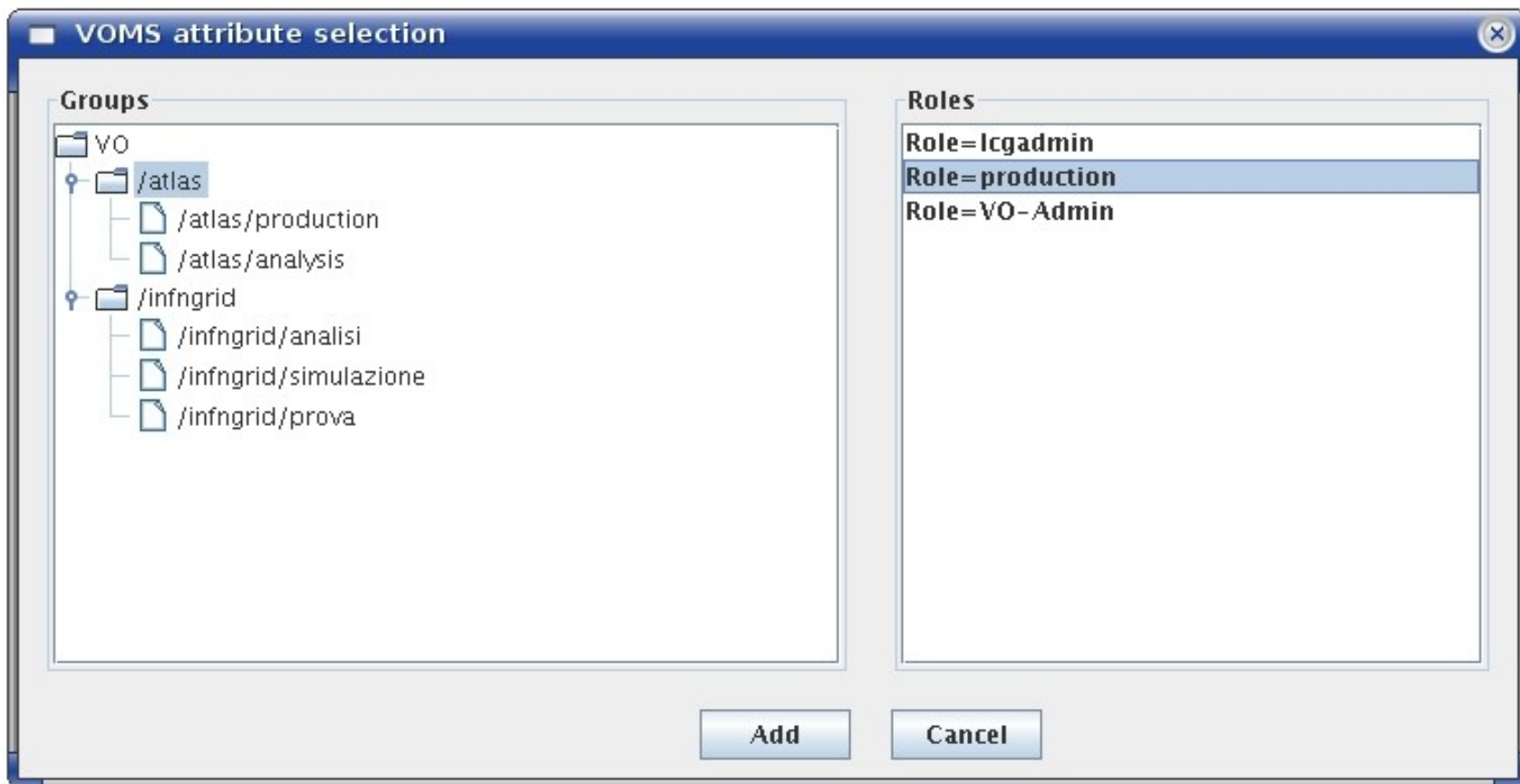
- Contains Site or VO policies
- *User*: local user (or poolname) assigned to the Share of the Batch system
- Policies inside map FQANs (and/or DNs) to local user accounts

- The “Map to ACRB” box is needed only for compatibility with the current Information System
- Policies created by VO admins can/must be distributed to Site G-PBoxes
- FQANs can be retrived directly from VOMS (Ask VOMS button)
- The policy is associated to a Share PolicySet
- Just leave the “Map to ACRB” box blank for policies used local in a Site



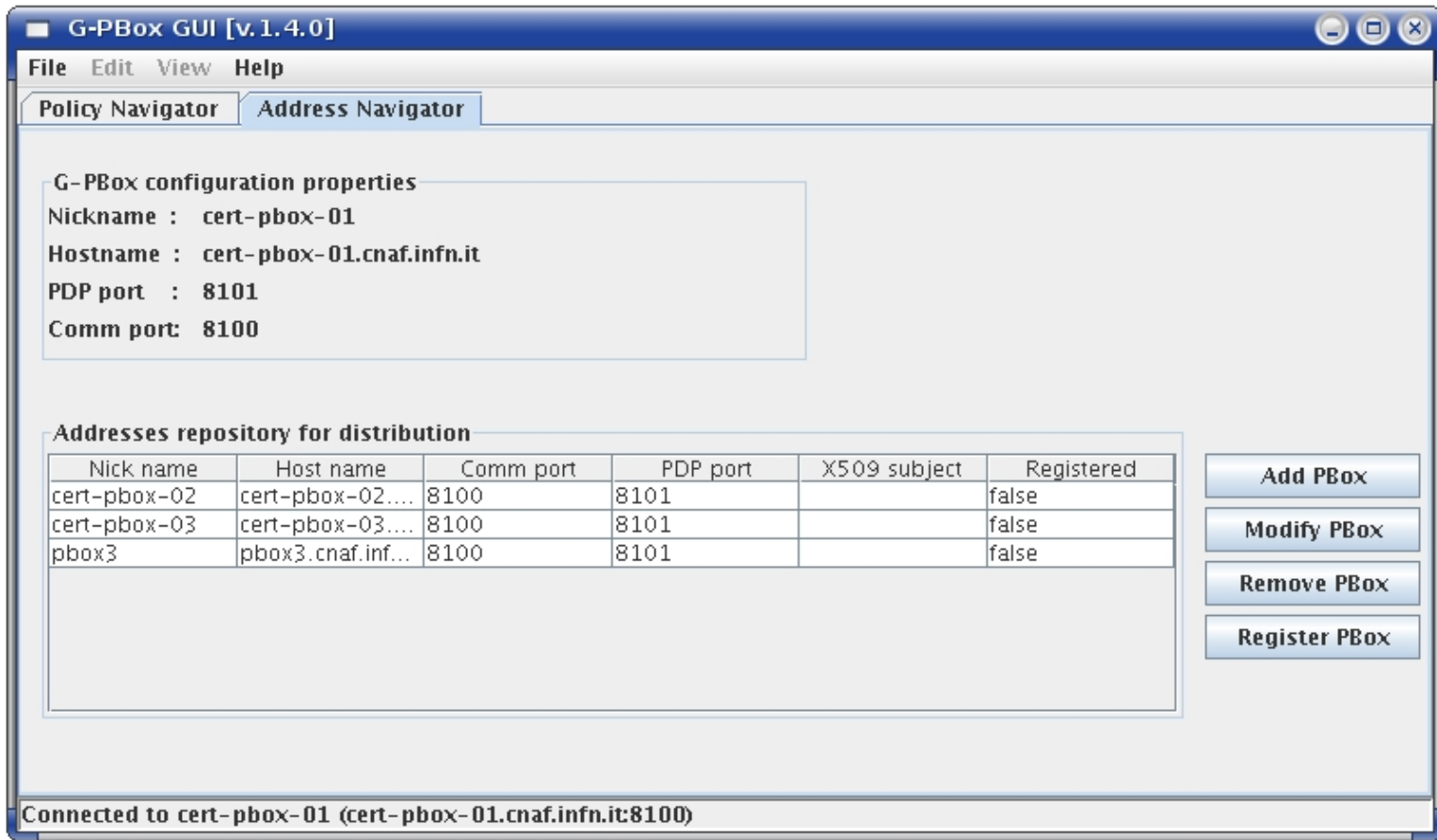
The screenshot shows a window titled "Create Policy - Wizard" with the following elements:

- Policy Id:
- Description:
- User DN:
- User FQAN:
- Map to ACRB:
- Buttons: "Ask VOMS", "Permit", "Deny", "Cancel"



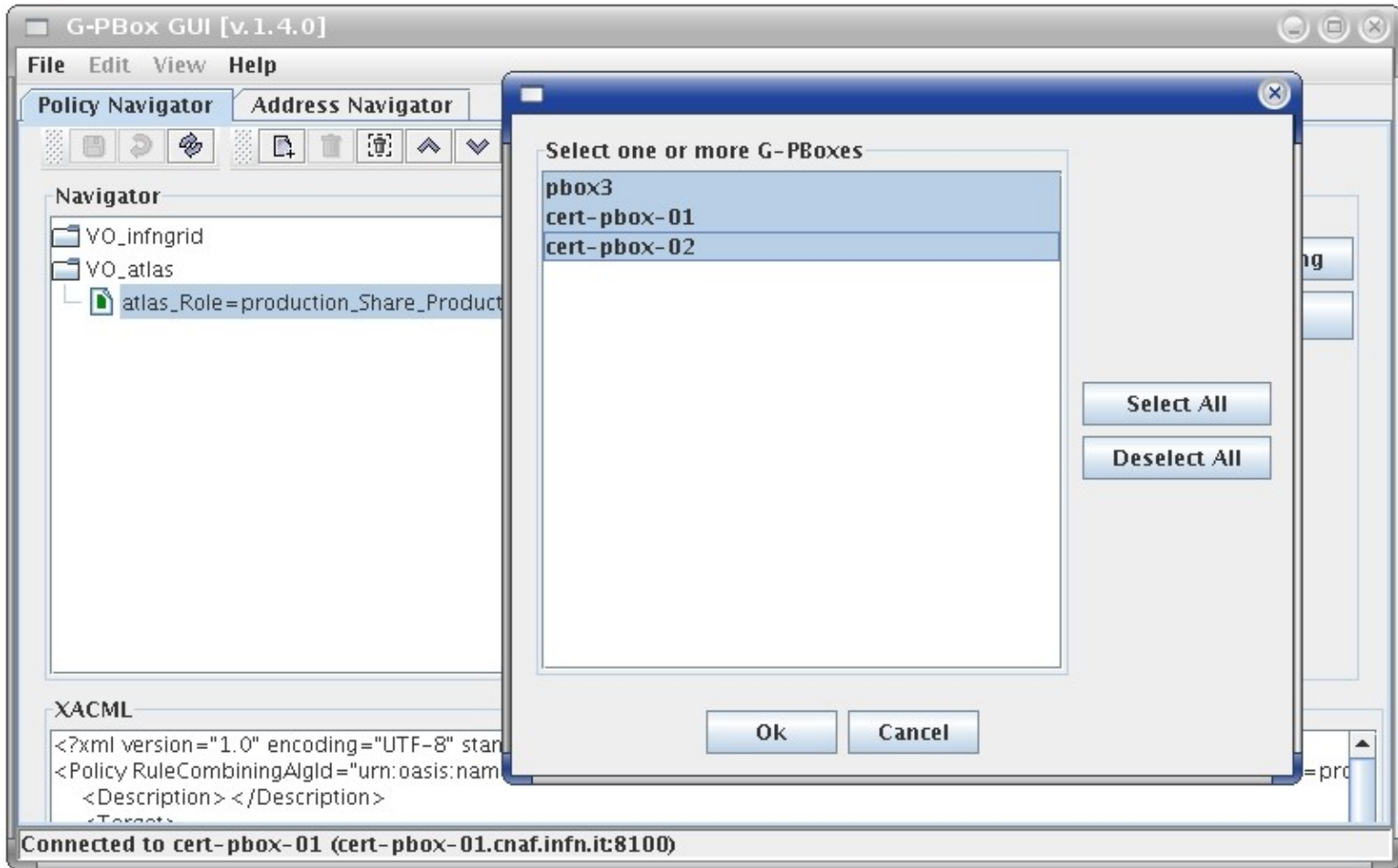
- **Used by the Create Policy wizard to retrieve FQANs directly from VOMS servers**
  - The selected group and/or role is added to the FQANs list
- **The VOMS servers are defined in a configuration file**

- **VO policies leverage information published into the Information System**
  - At the moment ***the only way*** to distinguish different shares is to use the ACBRs
  - ACBRs are authorization information and NOT resource characteristic information
  
- **The current GLUE schema lacks information on the CE side (characteristics of batch system shares)**
  
- **The next version (v2.0) of the GLUE schema will improve the description of the CE resource**
  - The batch system shares are going to be explicitly considered
  
- **Having Shares information in the IS drastically simplifies the “Create Policy” wizard**
  - The “Map to ACBRs” part of the Create Policy wizard will not be needed anymore



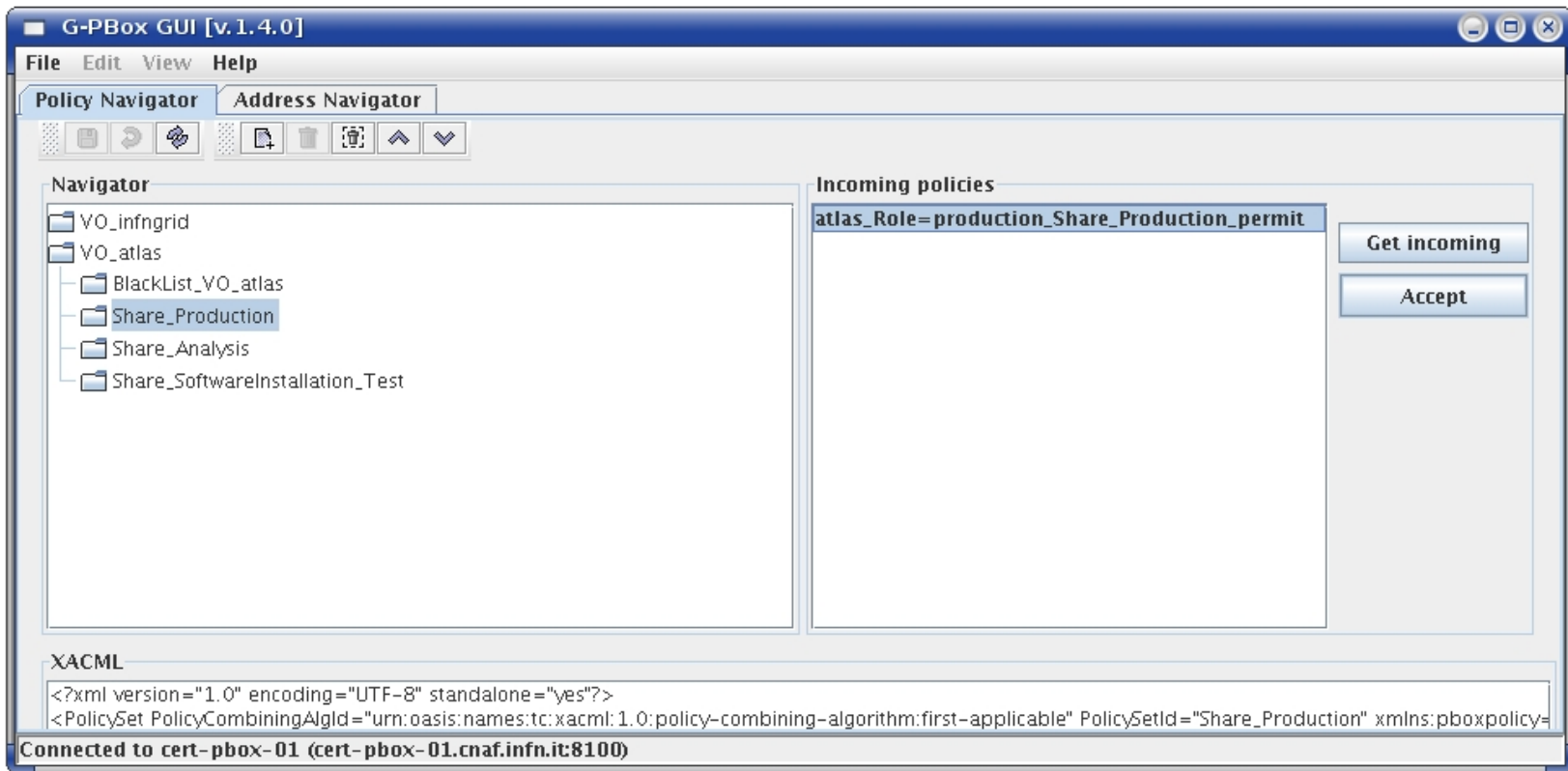
- Register the G-PBoxes involved in the Policy distribution

- **How distribution works now:**
  - The administrator selects a policy and sends that policy to a set of G-PBoxes
  - The administrators of the target G-PBoxes:
    - See new policies in the “Incoming policies box”
    - Accept the new policies and put these policies in the correct policy set
- **Next distribution development step:**
  - PolicySet-level synchronization among different G-PBoxes
    - Different synchronization modes based on the Master/Slave (Authoritative/Non Authoritative) concept
      - *Accept modifications with/without confirmation*



- **The VO administrator selects a policy and sends it to a set of Site G-PBoxes**





- **New policies have to be accepted and put in the correct PolicySet**

- **Short term**
  - GUI improvement
  - PolicySet synchronization mechanism
- **Long term**
  - ? (to be decided...)