

Security for AstroGrid

David Chadwick

d.w.chadwick@kent.ac.uk

AstroGrid Security Requirements

1. For access to the Virtual Observatory
2. For VO membership management
3. For access to the VO Space Repository
4. For spawning jobs to grid clusters

Overall Requirements

- Virtual Observatory providers set their own (fairly static) policies for who can have which types of access
- Organisations who make use of these services will dynamically control their own memberships of the Virtual Observatory Virtual Organisation (VOVO)

Virtual Observatory Access

1. The world wide community of privileged astronomers is dynamic and in a continual state of flux, but the observatories should not need to change their access control policies to cater for this
2. Implies access to an observatory should be role based, with a fixed number of trusted entities allowed to assign this role
3. Also implies that other trusted entities should be dynamically created i.e. there should be dynamic delegation of roles between organisation, countries, and VOs

VO Membership Management

- Different subsets of the astronomers in the world should have differing levels of access to the Virtual Observatory resources – implies we need different VOVO membership roles
- Only a subset of those holding Grid PMA certificates should have access to the Virtual Observatory – implies PKI certs on their own are not enough
- Membership of VOVO roles should be controlled locally by trusted local managers

VO Space Repository Access

- Only VOVO members should have write access to the repository
- Each VOVO member has his own storage allocation
- Implies access to a storage location should be based on the DN of the user
- VOVO member can set access rights on his own storage and give other members access to it
- Public can have read access to some data (depending upon the owner)

Spawning jobs to Grid Clusters

- User should be able to store a job's output and come back later to pick it up
- Implies job and its output should be linked to the DN of the user
- Permission to spawn a job should be given to a community of users, and should be linked back to user who spawned the job
- Job should run under local user name but be linked back to user who spawned the job

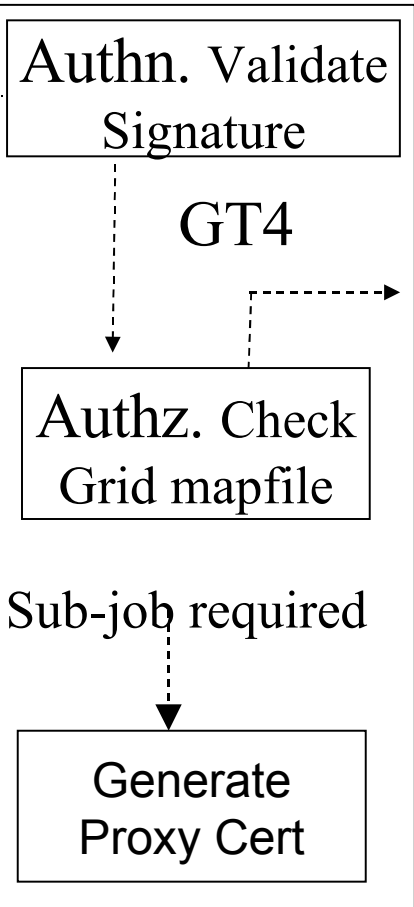
Outlining a Solution

- Proxy certs are a good basis to start from. They provide
 - User Authentication
 - Delegation from a user to a job and from the VO to a grid cluster, retaining the name of the original user
 - A means to package roles and push them from the user to the service provider
 - But NO authorisation on their own. Usually use grid mapfile
- Use MyProxy for roaming users
- Need a mechanism for assigning roles to users
 - VOMS is one way of doing this, and will package the user roles in proxy certs for pushing (VOMS proxy init)
- Need a dynamic delegation of roles capability so that new role issuers can be dynamically created
 - PERMIS is one way of doing this since it supports validation of Attribute Certificate chains
- Add Shibboleth SSO later for users who don't have grid certs
 - Shebangs project from Man Uni should provide a solution here

Proxy Certs

(Proxy private key stored locally)

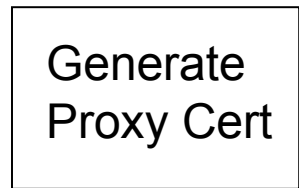
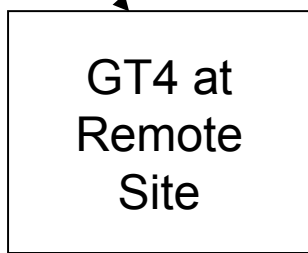
Submit
Grid job
(Mutual SSL
Authn contains
proxy certificate
chain)



Access
Request

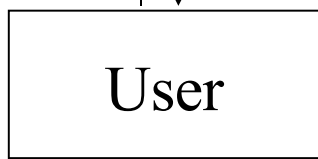


Submit Spawned Job



grid-proxy-init

Sign Proxy

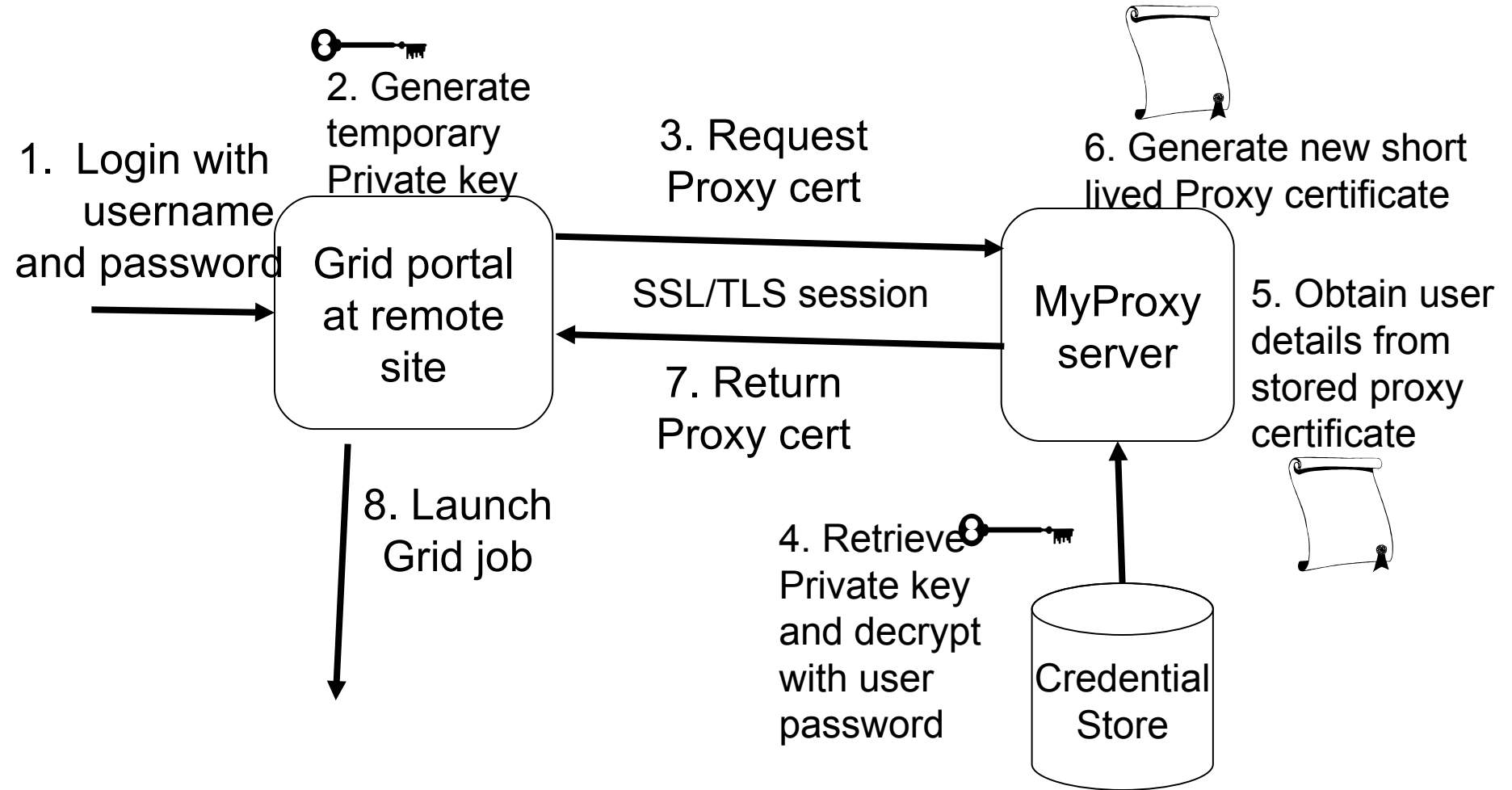


(Long term private key stored securely)

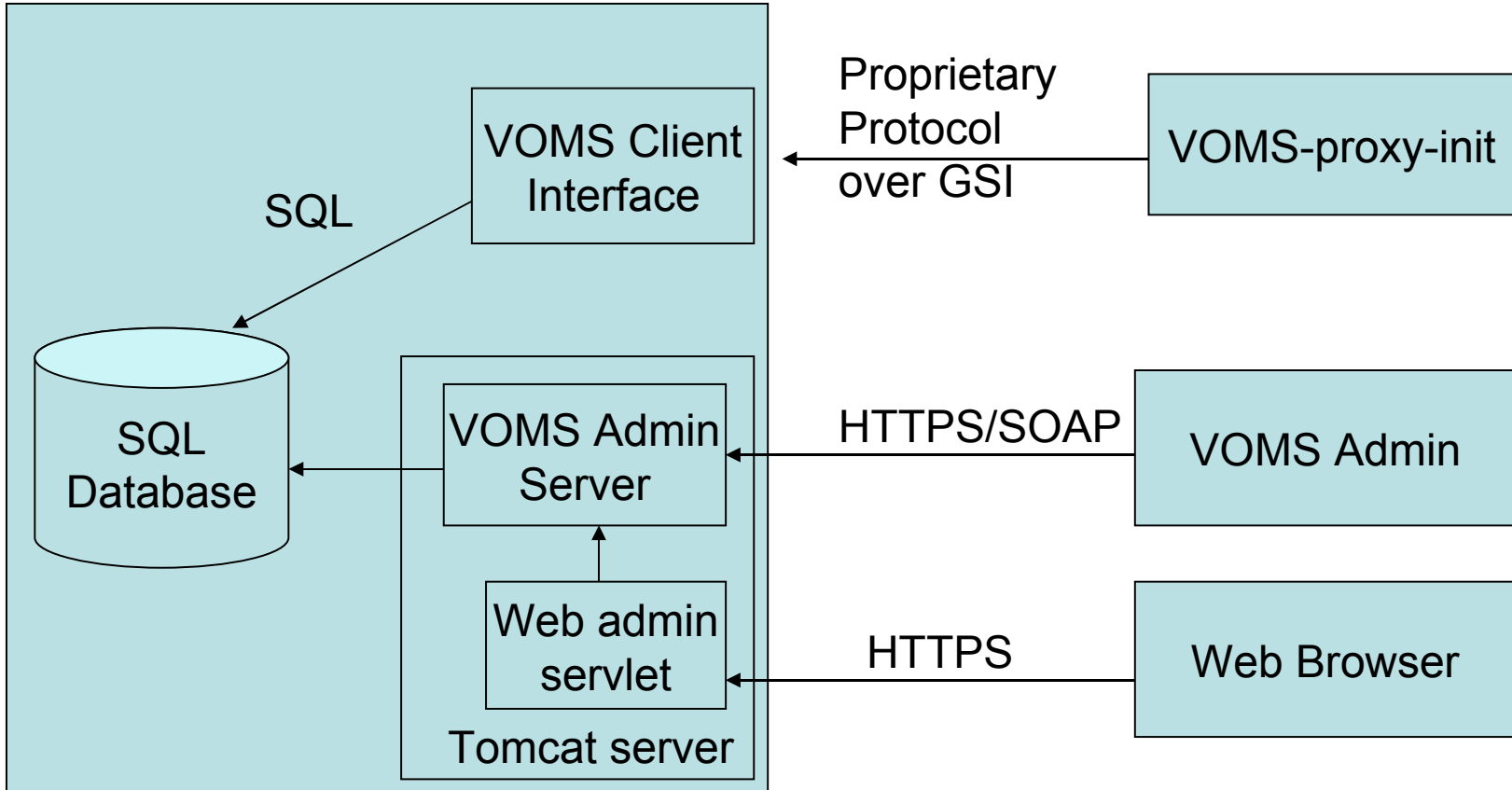
Sign Proxy



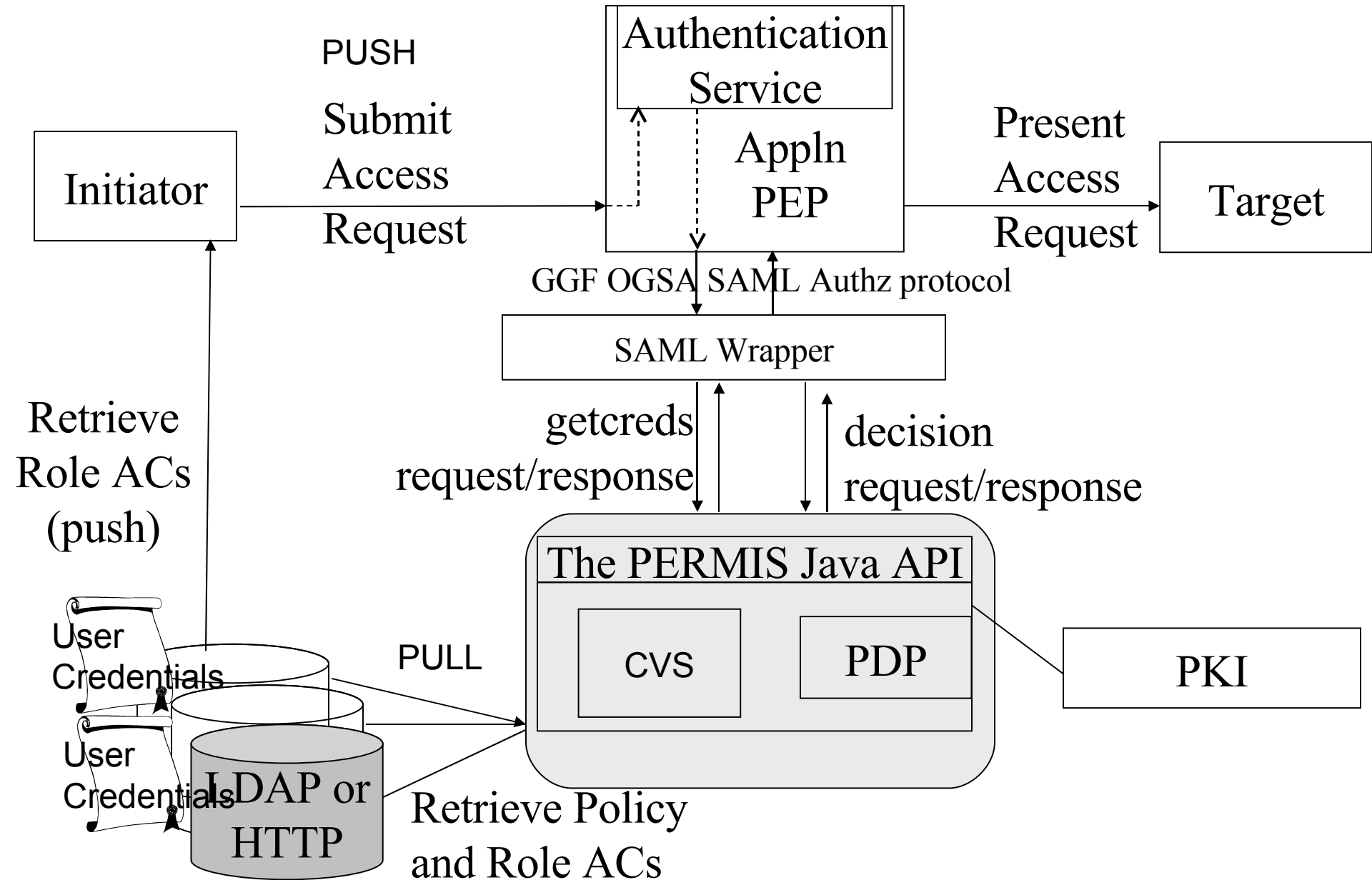
My Proxy



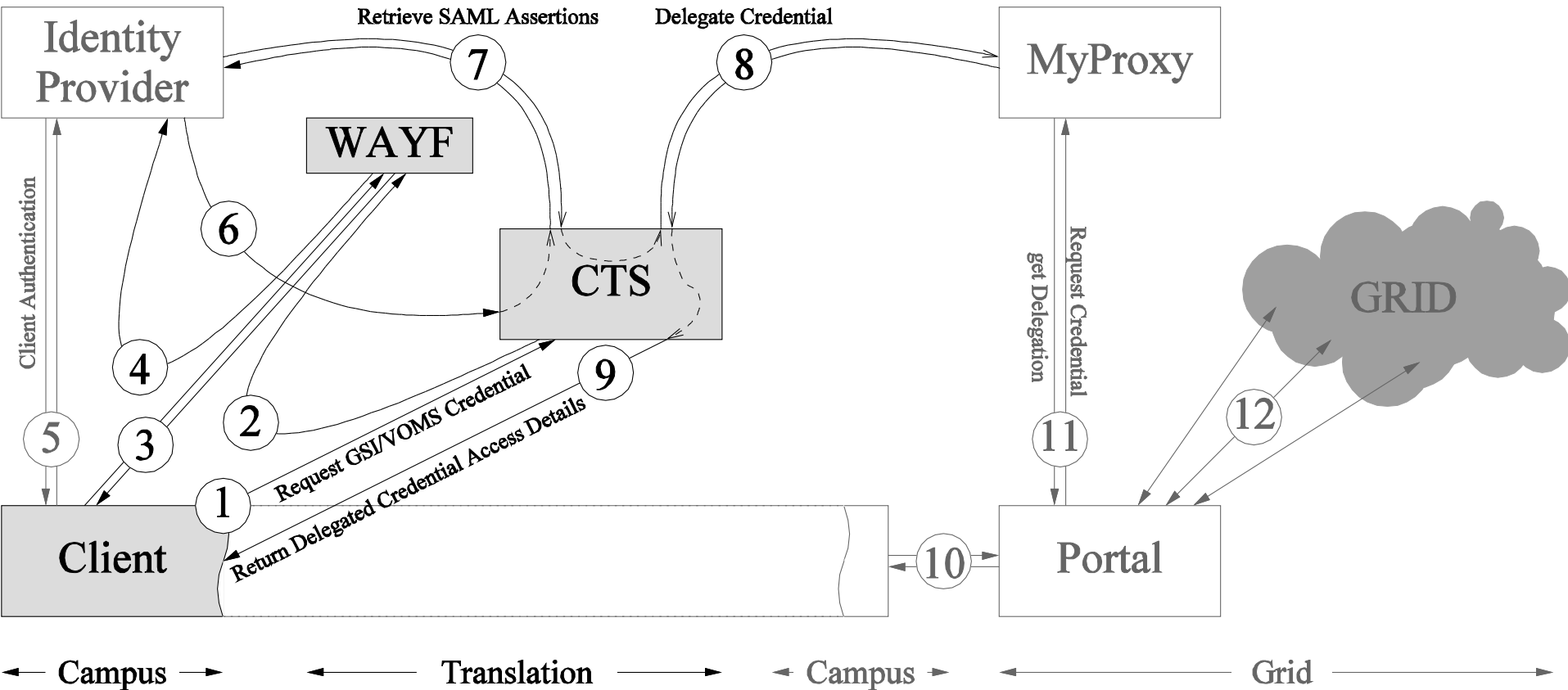
VOMS



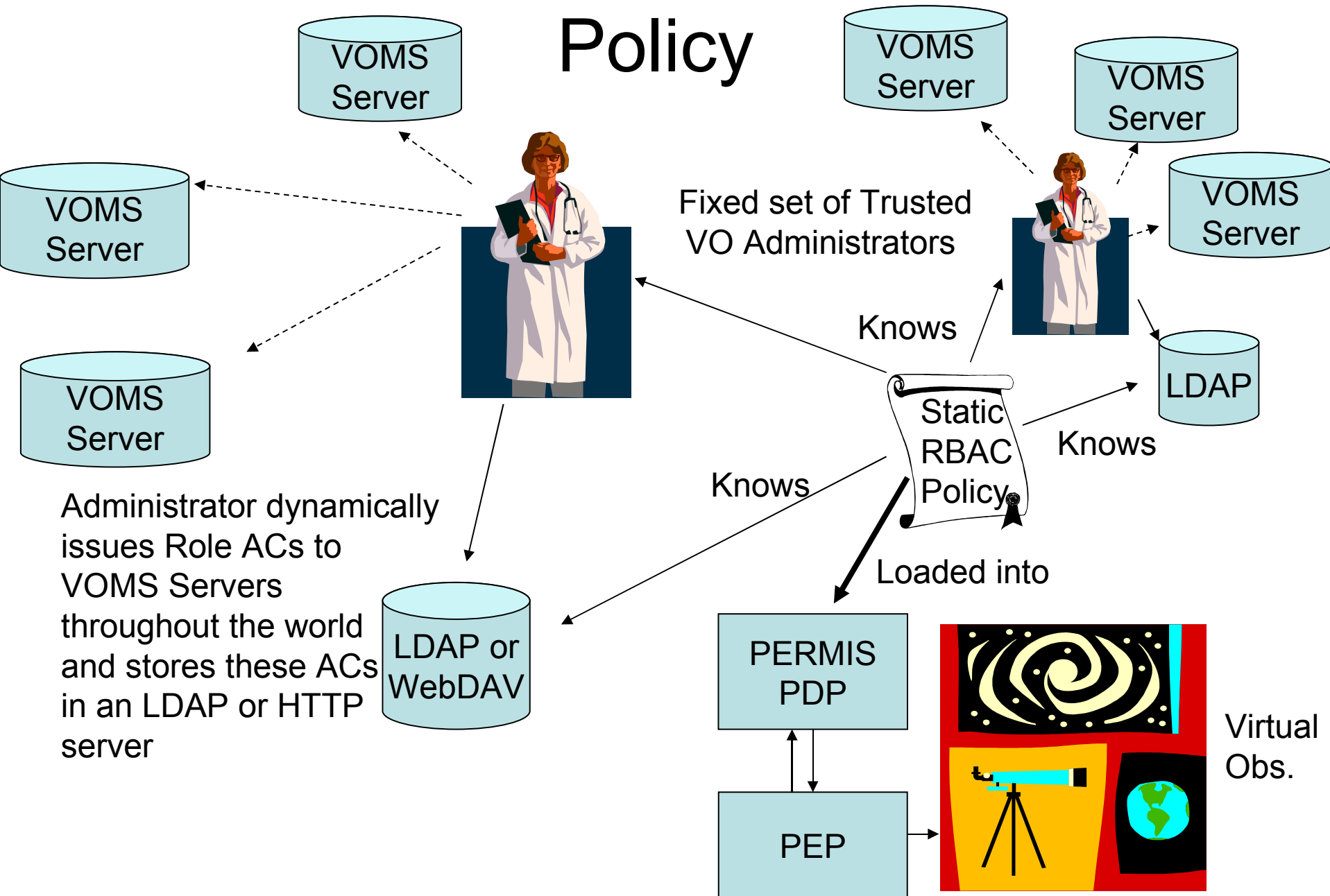
PERMIS Authorisation



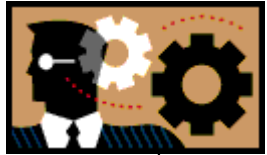
SHEBANGS Architecture



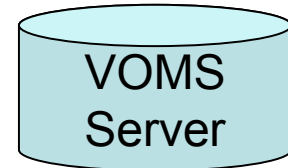
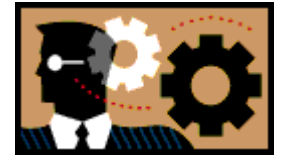
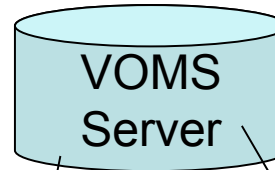
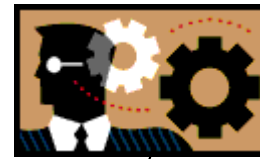
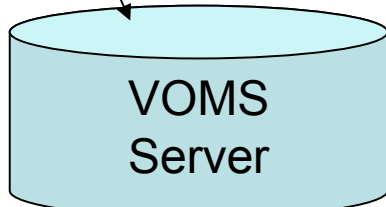
Setting Up the Virtual Observatory



Administering the Virtual Observatory Users



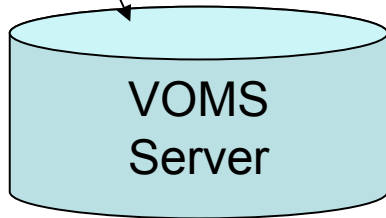
Local administrators
assigns roles to their local users



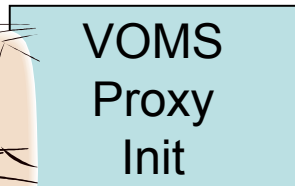
Accessing the Virtual Observatory



Local administrator assigns roles to users



Get Role AC embedded in proxy cert

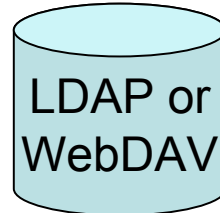


Astronomer



Trusted VO Administrator

Dynamically issues Role ACs to VOMS servers

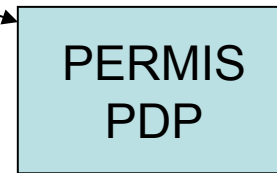


Pulls Role AC of VOMS Server

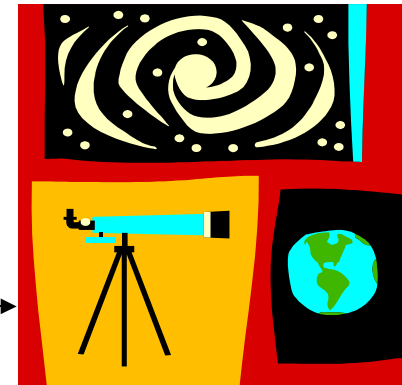
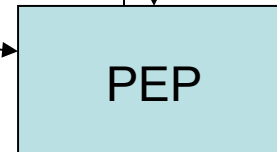


PERMIS PDP is capable of validating chains of role ACs

Loads



Proxy cert containing Role AC



VO

Accessing the Space Repository

