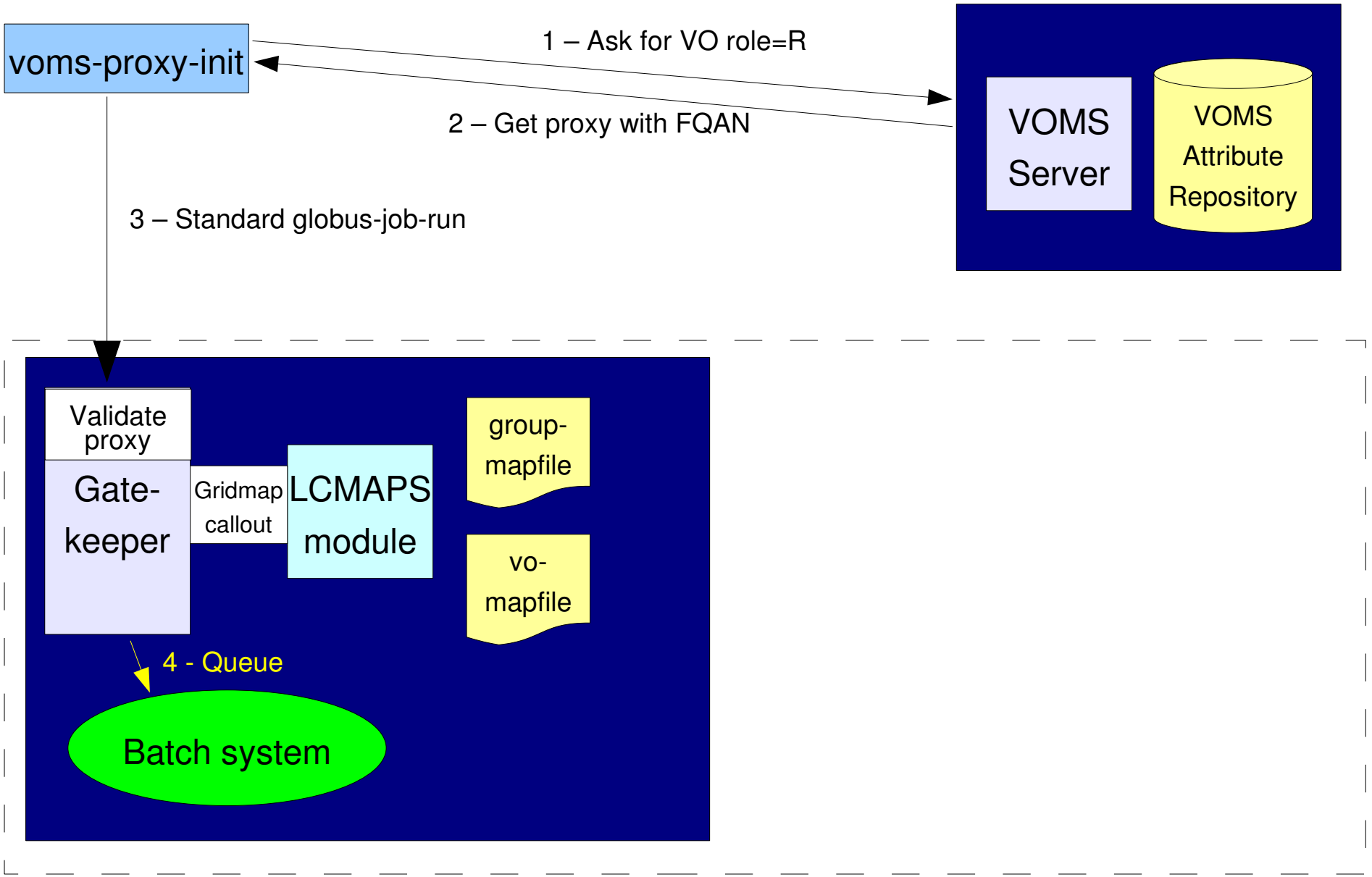
gLite Authentication

The way I understand it

by Igor Sfiligoi

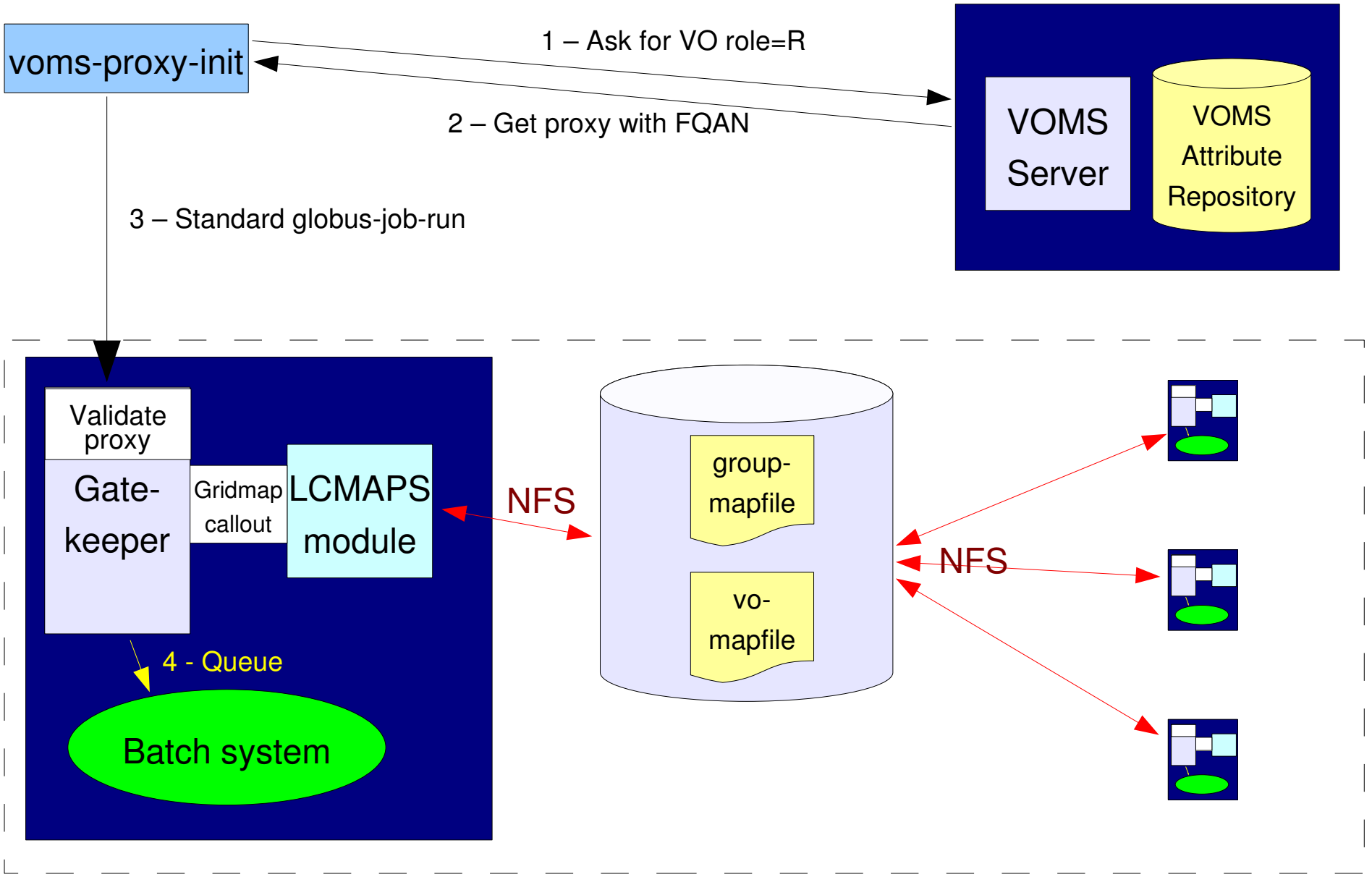
Current deployment



Implementation details

- Use grid-mapfile for legacy, non-VOMS users
- Use FQAN-only mapping for group and pool accounts
  - For example: /atlas/* -> atlasXXX
- Use all FQANs of a proxy to map secondary GIDs
  - A user may be mapped to (UCMS1,GCMSPROD) and have a second GID=GLCGPROD
- Everything is disk based

Proposed short term plan



Multiple PEPs

- They never really addressed the problem
- The current solution works with NFS shared disk space
  - Very low security
  - May not scale when using gLExec on WNs
- They do plan to create a centralized PDP
  - Much like GUMS

Why they don't use GUMS?

- Not developed in Europe ;) (just kidding)
- Privacy laws
  - GUMS keeps DNs of users that never submitted to site
- Missing functionality
  - Multiple FQANs
- PRIMA-GUMS implementation
  - Prima currently does not verify the FQAN signature and relies solely on GUMS mapping for refusal

Can GUMS be modified to suit them?

- Possibly... if PRIMA get changed
  - If DN/FQANs are not collected from VOMSes, someone must verify FQAN signature
- Three solutions to the above problem:
  a) VOMS public keys everywhere
  b) An authentication service
  c) GUMS gets the full proxy and verifies it (no SAML)
- Option b) seems the most appealing

Timeline

- None
- Still discussing if this is something we want to pursue or not