OSG Site Administrators Workshop

Using gLExec to improve security of Grid jobs

by

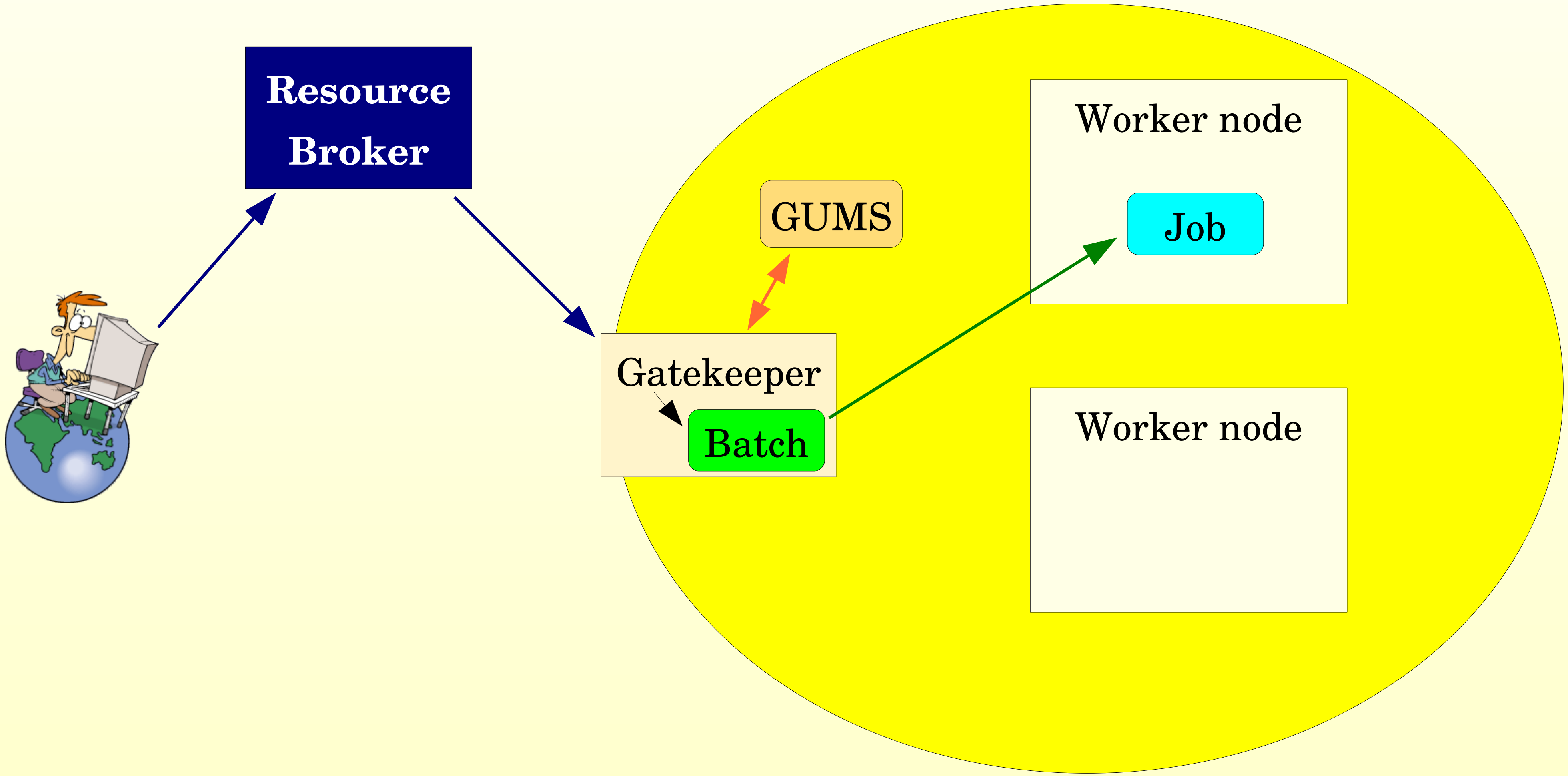
Alain Roy and Igor Sfiligoi

Outline

- Why do we need gLExec
- How does gLExec work
- Conclusions

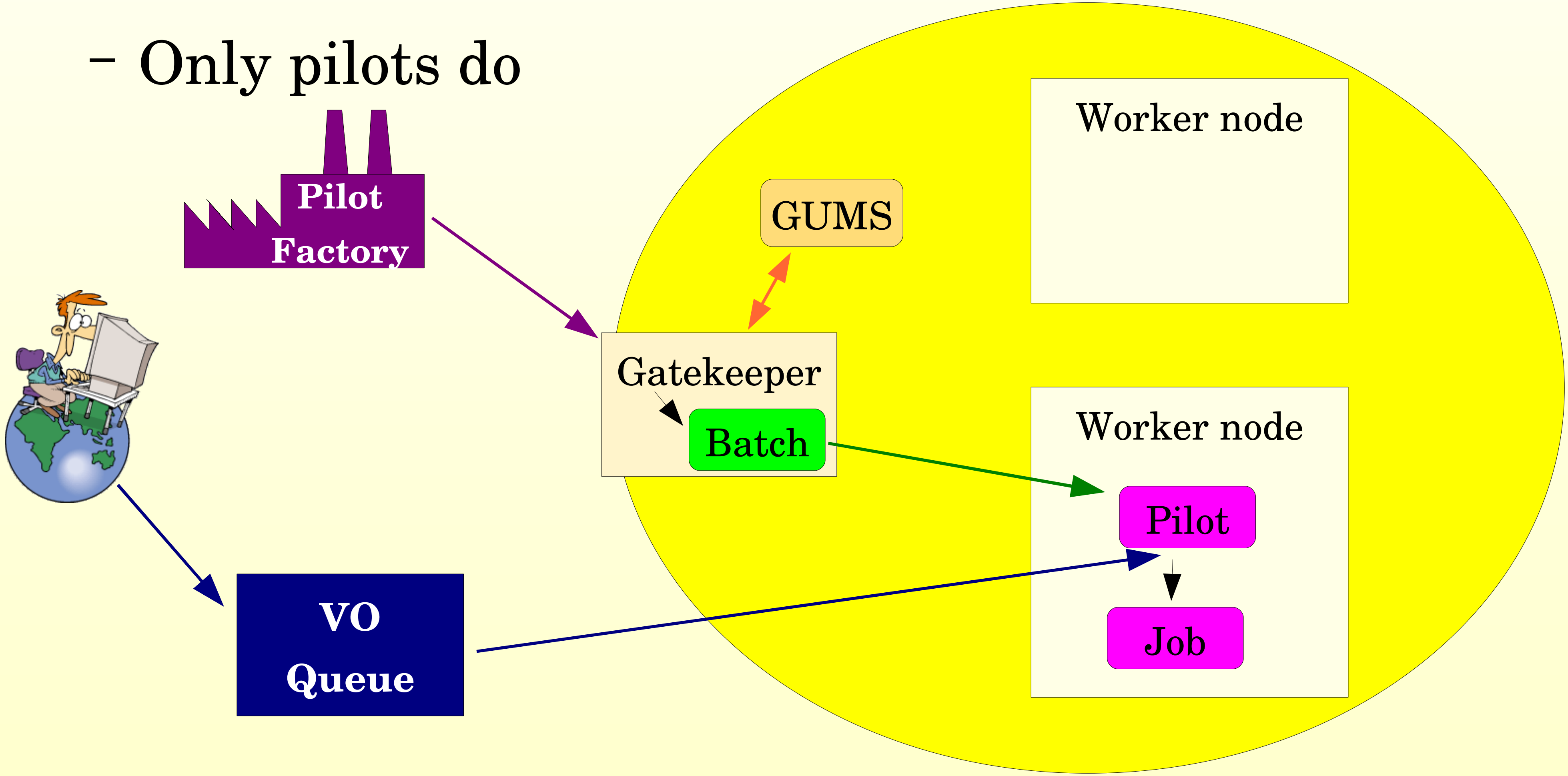
Traditional Grid Jobs

- User jobs come through the Gatekeeper



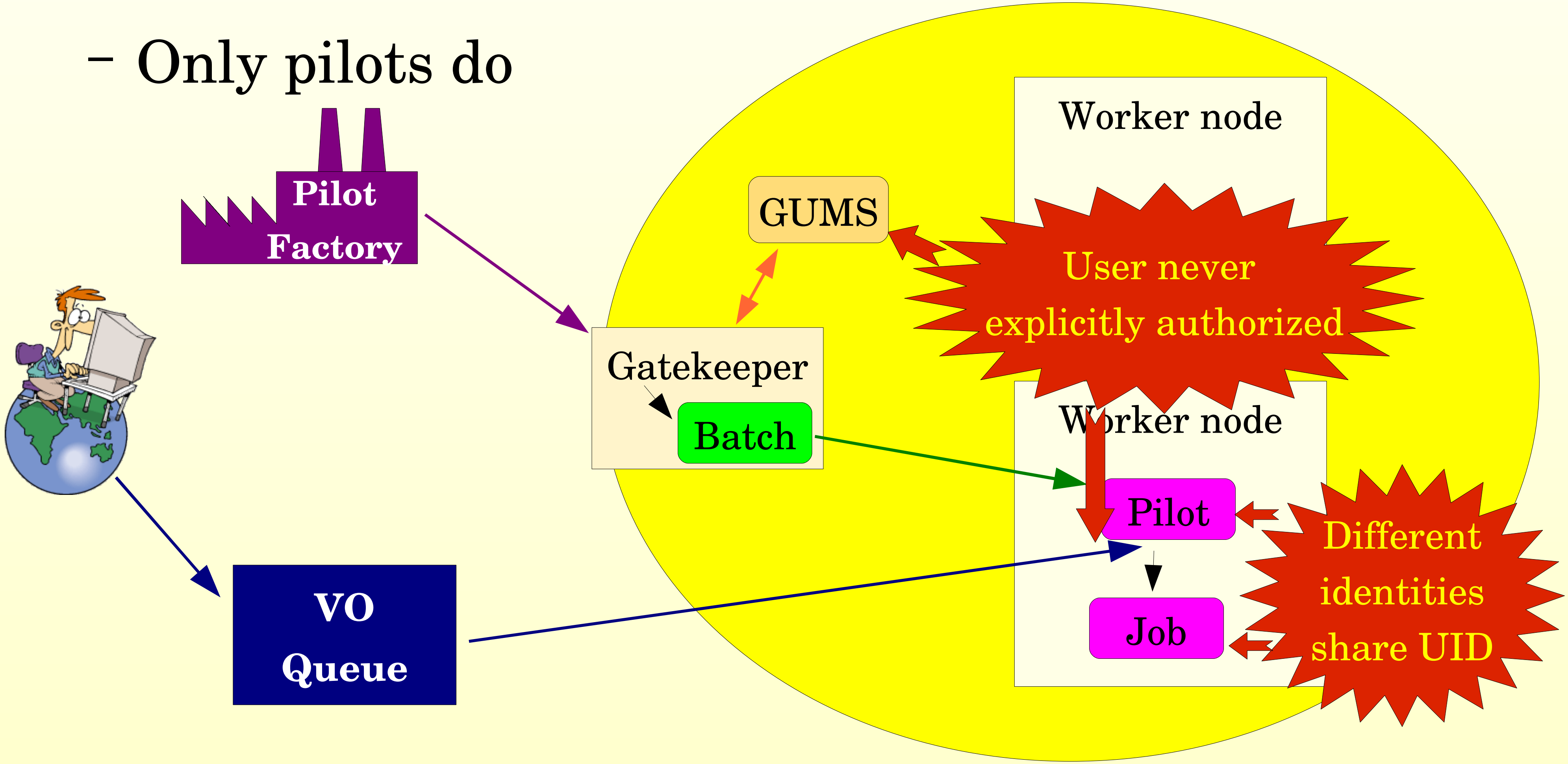
Pilot Grid Jobs

- User jobs **don't** come through the Gatekeeper
  - Only pilots do



Pilot Grid Jobs (2)

- User jobs **don't** come through the Gatekeeper
  - Only pilots do

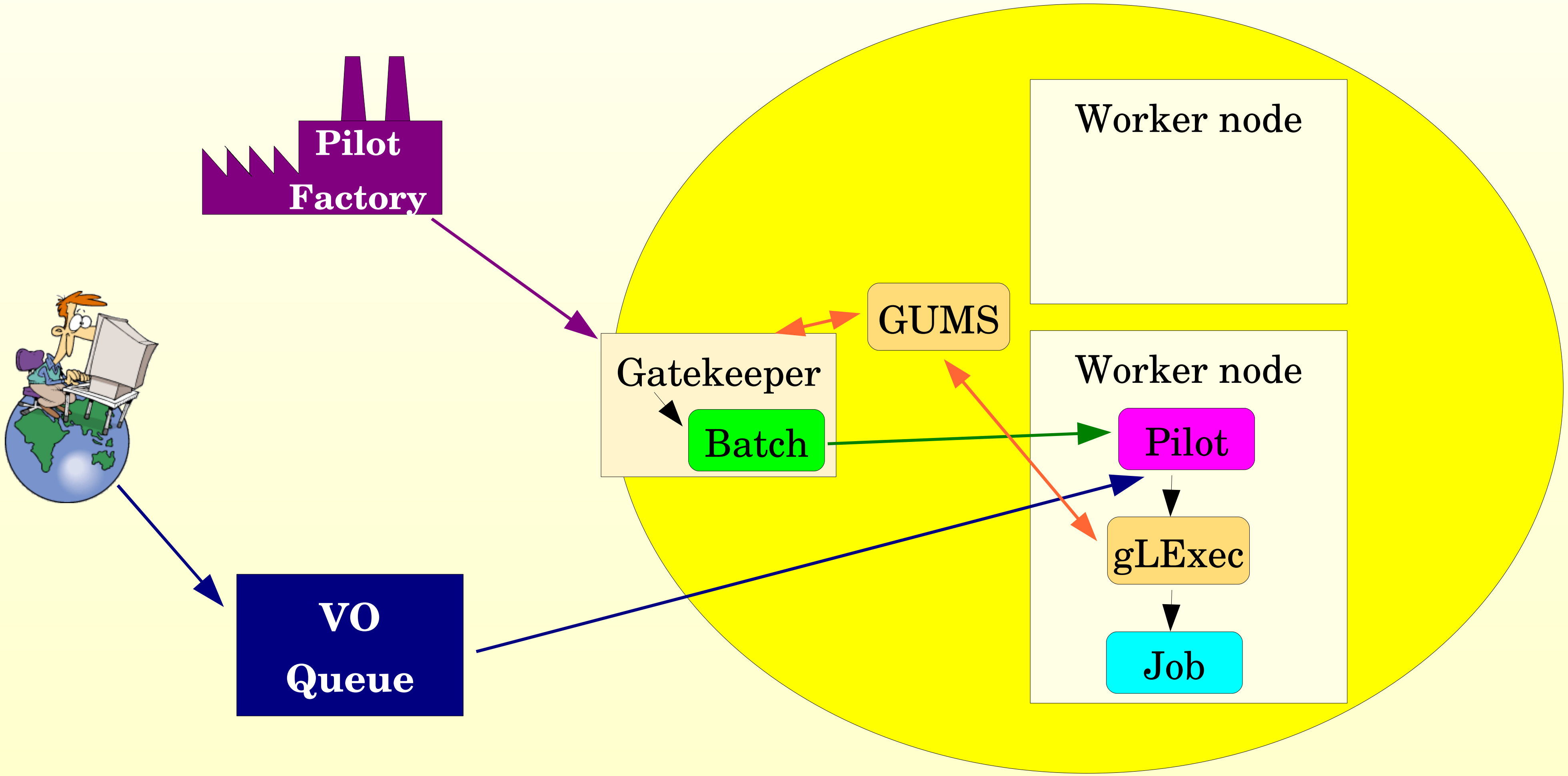


Pilot jobs in use today

- Several VOs are actively using Pilot jobs
  - CDF
  - ATLAS
- Others are about to start using them
  - CMS
  - MINOS
- Pilot jobs are here to stay

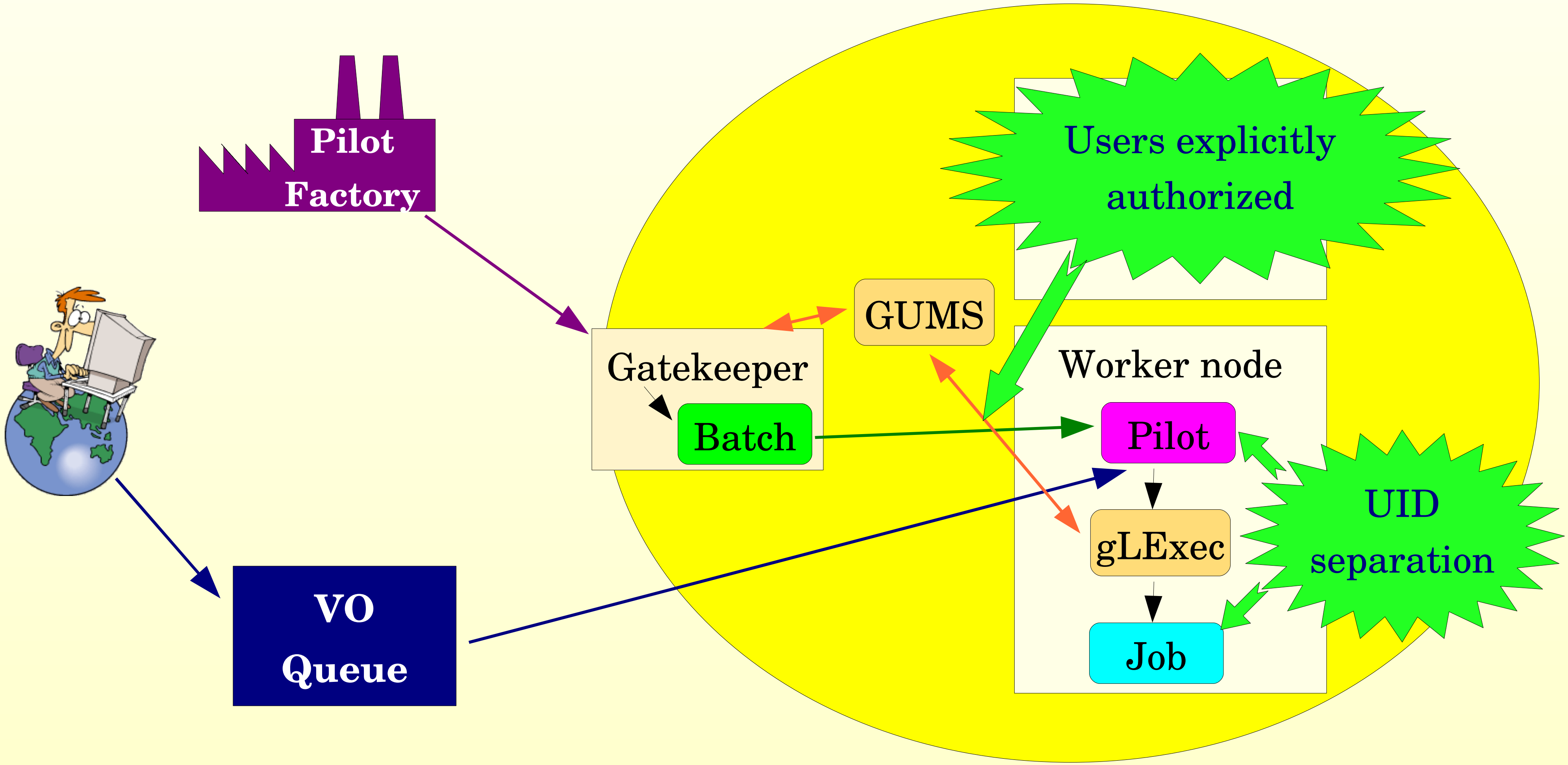
Pilot Grid Jobs with gLExec

- User jobs started using gLExec



Pilot Grid Jobs with gLExec (2)

- User jobs started using gLExec



What is gLExec

- A Grid-aware suExec derivative
  - Allows execution of commands as a different user
  - Authorization and mapping based on x509 proxy
- A privileged executable
  - Needed to switch identities
- Pluggable architecture
  - PRIMA/GUMS plugin used by default in OSG

gLExec IS a privileged executable

- gLExec is NOT a privileged service
  - Not listening on any network port
- gLExec is a privileged executable
  - Will run as root at least part of the time
  - A bug can potentially give an attacher root privileges
- gLExec has been audited by EGEE for potential security problems
  - None have been found

gLExec and accounting

- gLExec keeps detailed logs of each invocation, including
  - user DN and FQAN
  - start and stop times
  - process id
- A gLExec GRATIA probe exists for automatic accounting extraction
  - but logs are also human readable

gLExec and Pilots

- Pilots need to be gLExec-aware
  - Pilots cannot be forced to use gLExec
- Using gLExec is in the best interest of pilots
  - Protects them from malicious users (UID switching)
- But if gLExec is installed, site can require its use by policy

gLExec installation

- gLExec supported by OSG
  - distributed via VDT
- Needs to be installed on all the worker nodes
- Requires host certificate or service proxy to talk to GUMS

For more details, see talk in the "Configuring OSG" session

Conclusions

- Pilot jobs are gaining momentum
  - Most big VOs (do or will) use them
- gLExec helps restore security for pilot jobs
- It is a privileged executable
  - But security benefits overweight risks
- Supported by OSG
  - Distributed in VDT