New Authorization Service

Christoph Witzig, SWITCH

(christoph.witzig@switch.ch)

MWSG March 27, 2008

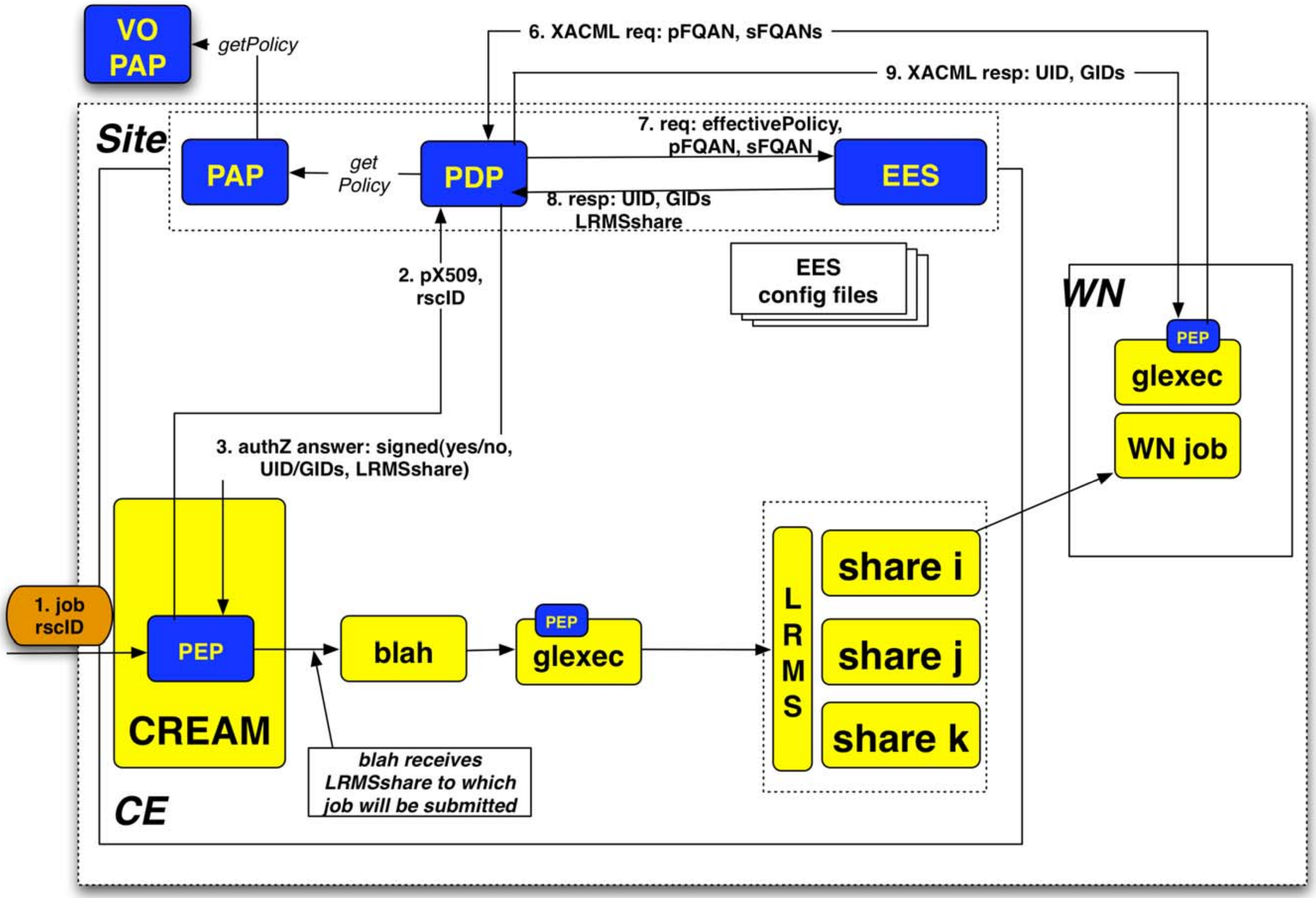
New authZ Service

- **Work item in EGEE-III for CNAF, HIP, NIKHEF and SWITCH**
  - CNAF: 6PM, HIP: 6PM, NIKHEF: 18PM, SWITCH: 12PM
- **Requirements:**
  - Uniform authorization and policy management in gLite
  - Compatible with SAML and XACML standards
  - Built on the experience of previous systems
    - LCAS/LCMAPS, SCAS, G-PBox, gJAF
  - Not constrained to the use of any existing implementation
    - though recommended for the sake of economy
  - Development and deployment within EGEE-III
- **Relation to SCAS**
  - addresses the problem of gLexec on the WN on a short time scale
  - Calling LCAS/LCMAPS over the network
- **Focus on job management**

Functional Components

- **PEP: Policy Enforcement Point**
    - for Java and C
- **PAP: Policy Administration Point**
    - Administration for local policies
    - Obtain and merge remote policies
- **PDP: Policy Decision Point**
    - XACML-SAML profile
- **EES: Execution Environment Service**
    - Returns the local environment within which the job will run
    - Examples: UID/GIDs, work space, virtual machine

High Level Design


VO PAP
getPolicy
6. XACML req: pFQAN, sFQANs
9. XACML resp: UID, GIDs
Site
PAP
get Policy
PDP
7. req: effectivePolicy, pFQAN, sFQAN
EES
8. resp: UID, GIDs LRMSshare
2. pX509, rscID
EES config files
WN
PEP
glexec
WN job
3. authZ answer: signed(yes/no, UID/GIDs, LRMSshare)
1. job rscID
PEP
CREAM
blah
PEP
glexec
L R M S
share i
share j
share k
blah receives LRMSshare to which job will be submitted
CE

Benefits of new authZ Service (1/2)

- **Clear separation of responsibilities of VO policies and site configuration**
  - VO policies may be overridden by site managers
- **Allows remote client to obtain authorization policy at a the site as needed**
- **Use of XACML allows more complex authorization policies**
  - Note: XACML language must be hidden from (average) VO and site administrators
- **Site administrator retains full control of Execution Environment**
- **Execution Environment Service shall be extensible to allow for other execution environments than just UID/GIDs**

Benefits of new authZ Service (2/2)

- **“FQAN - share decoupling” should be a configurable option from the authorization point of view**
  - Clearly this goes beyond only authorization
- **Lay the groundwork for credentials other than X.509**
- **Interfaces capitalize on common work between EGEE, OSG and Globus**
  - SAML-XACML profile
  - Consider to use same interfaces as Globus authorization framework
- **Aim for minimal dependencies**
  - standalone installation must be possible
  - Individual components should be deployable in other configurations/middleware
- **Simple command line debugging tools**

Timeline

- Currently working on detailed design of components
- May 08: Initial Working Design finished
- Dec 08: First version
- Summer 09: in deployment