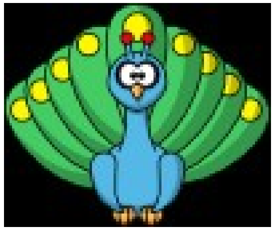
Argus: gLite Authorization Service



Overview

Christoph Witzig, SWITCH
(christoph.witzig@switch.ch)

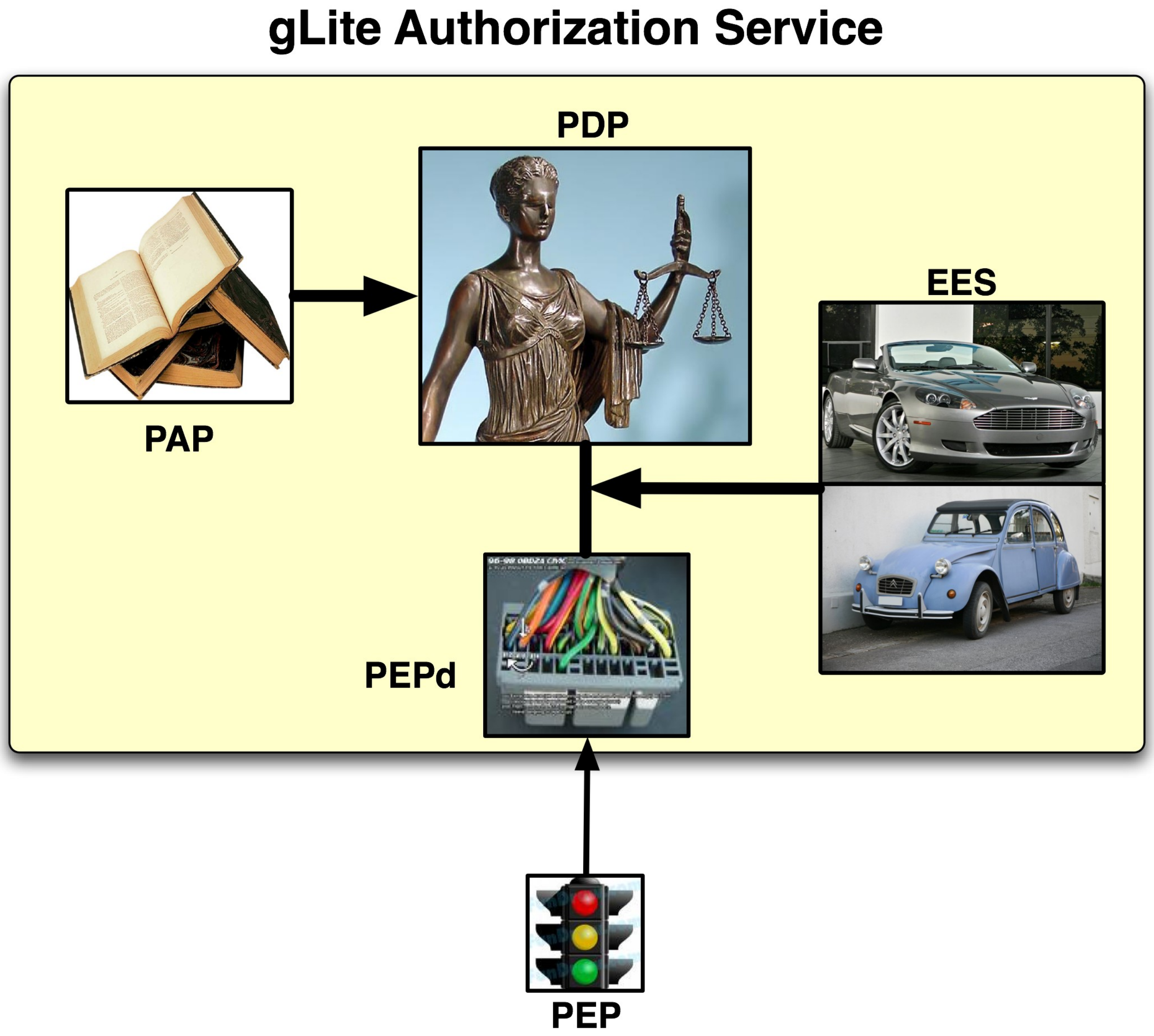
www.eu-egee.org

Information Society and Media

Outline

- Introduction and supported use-cases
- Mid-term work
- Appendix: Motivation for Argus

Architecture



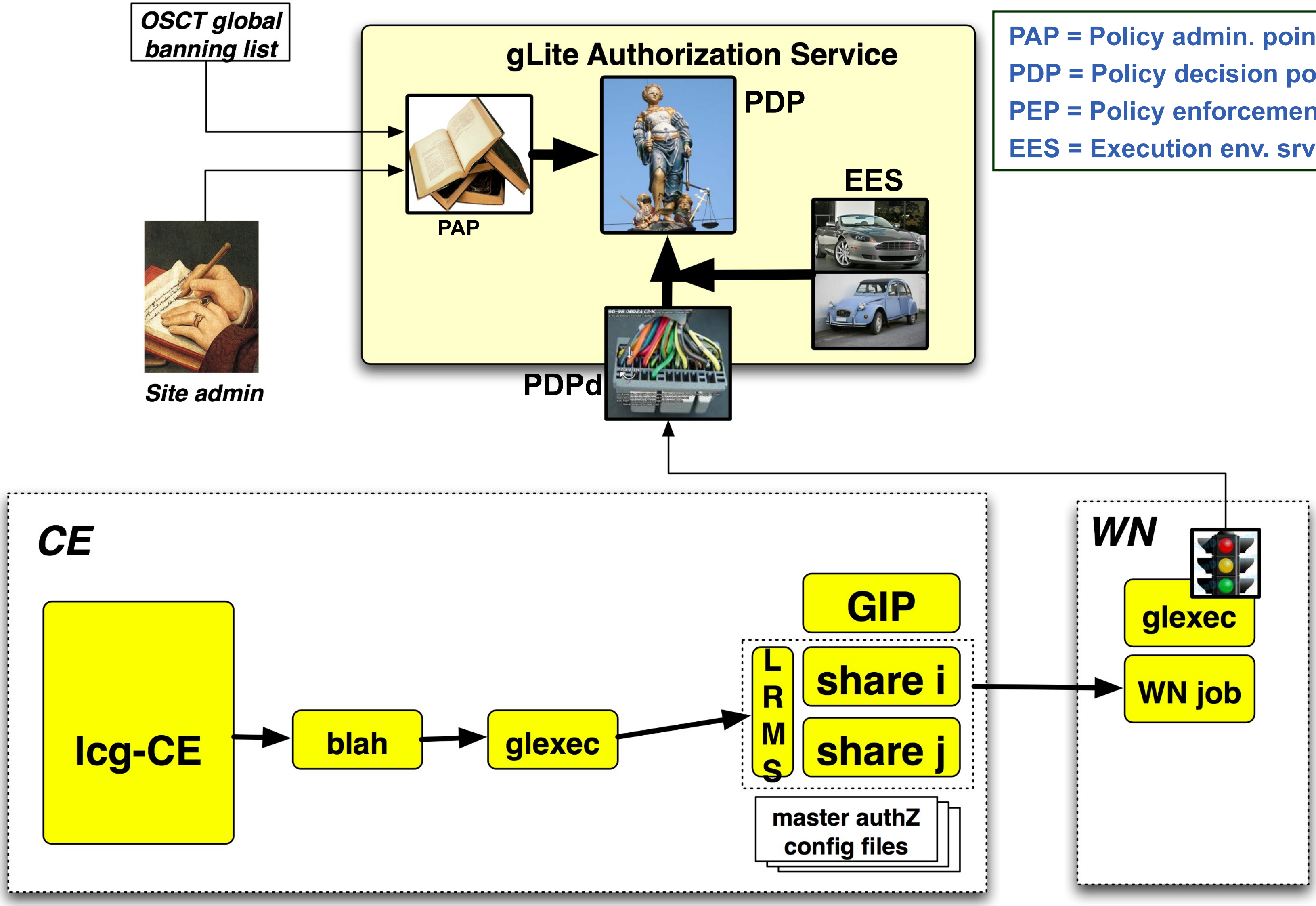
Argus PT

- **Institutions involved:**
  - CNAF: PAP
  - HIP: certification and test-bed
  - NIKHEF: EES
  - SWITCH: PDP and PEP daemon
  - Leading institution: SWITCH

- **Organized as Argus PT**

Currently Supported Deployment (1/2)

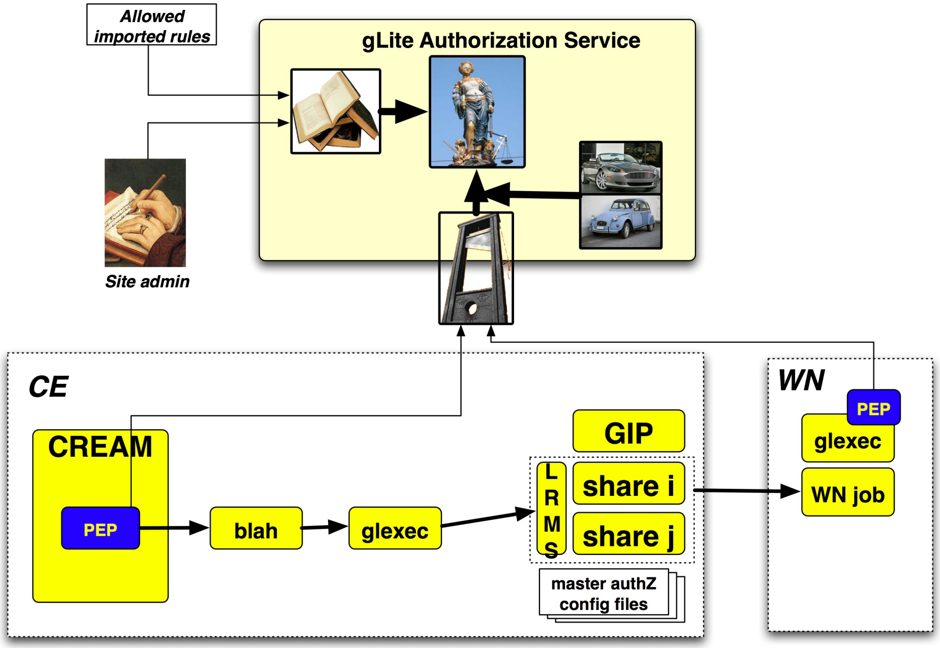
PAP = Policy admin. point
PDP = Policy decision point
PEP = Policy enforcement point
EES = Execution env. srv



Currently Supported Deployment (2/2)

- **Supported today:**
  - Glexec on WN
  - Global banning (PAP operated by OSCT / EGI CSIRT)
  - GSI PEP callout (→ gridFTP)

- **Work in progress: CREAM integration**



Near and Mid-term Features

- **Shared filesystem:**
  - Today: No shared filesystem needed for deployment on *single* host
  - Coming feature: Deployment on multiple-hosts will be supported without the need for a shared filesystem (in memory replication of mappings)

- **XACML policies**
  - Rich feature of XACML policies
    - Today: use only a small subset (which is OK, but we have the means to make it more elaborate if needed)
  - Easy to add new attributes
  - Namespace: common namespace proposed: urn.mace.xyz

- **EES**
  - Support for more complex execution environments

Mid-term Issues

- **Argus is happy to support other CEs**
  - ARC, UNICORE?
  - First step: write profile (example https://edms.cern.ch/document/1058175/1.0.1)
- **Data management:**
  - Held preliminary discussions with DM
  - Study planned in summer/fall to clarify use-cases and devise plan
- **Main goal: Single point for authorization configuration at a site**

Further Information

- **About the service:**
  - authZ service design document: https://edms.cern.ch/document/944192/1
  - Deployment plan: https://edms.cern.ch/document/984088/1
- **General EGEE grid security:**
  - Authorization study: https://edms.cern.ch/document/887174/1
  - gLite security: architecture: https://edms.cern.ch/document/935451/2
- **Other:**
  - Wiki:
    - https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework
  - EGEE08 presentations:
    - http://indico.cern.ch/sessionDisplay.py?sessionId=94&confId=32220
    - http://indico.cern.ch/sessionDisplay.py?sessionId=95&slotId=0&confId=32220 - 2008-09-25

Appendix

Motivation for Argus

Motivation:

Which Problems Are We Trying to Solve?

- **Different Services use different authorization mechanisms**
- **Some services even use internally more than one authorization framework**
- **Site administrators do not have simple debugging tools to check and understand their authorization configuration**
- **Site administrators must configure the authorization for each service at their site separately**
  - Consequence 1: At a site, there is no single point to ban users/groups of users for the entire site
  - Consequence 2: many site administrators don’t know how to ban users
  - There should be a command line tool for banning and un-banning users at a site

Motivation:
Which Problems Are We Trying to Solve?

- **There is no central grid-wide banning list to be used during incidents**
  - Consequence: Urgent ban cannot be taken for granted during incidents
- **Sites cannot publish their complete authorization policy to the outside world**
  - Currently only assignment of FQANS (experience of DENY tags)
  - Note: Fixing this problem does not mean that sites MUST publish their authorization policy
- **No monitoring on authorization decisions**

Motivation:
Benefits of the Authorization Service (1/2)

- **Main benefit within EGEE-III:**
  - Addressing the above list of short-comings

- **In addition:**
  - Resistance to failure and simple means for scaling the service
    - Flexible deployment model
    - No dependency on a shared file system
    - High availability option
  - Client component is very lightweight
    - Small amount of code
    - Few dependencies (especially on WN)
    - Portability: support on other OS and languages easy

Motivation:
Benefits of the Authorization Service (2/2)

- **In addition (cont.):**
  - Enables/eases various authorization tasks:
    - Banning of users (VO, WMS, site, or grid wide)
    - Composition of policies – CERN policy + experiment policy + CE policy + OCST policy + NGI policy=> Effective policy
    - Support for authorization based on more detailed information about the job, action, and execution environment
    - Support for authorization based on attributes other than FQAN
    - Support for multiple credential formats (not just X.509)
  - Support for multiple types of execution environments
    - Virtual machines, workspaces, …
  - Nagios plug-ins provided for monitoring of service