gLite Java Authorisation Framework (gJAF)

- extension of the test suite and a new VOMS generic attributes PDP

Trygve Aspelien and Yuri Demchenko
University of Bergen and University of Amsterdam

All-Hands meeting
June 18-20, 2007, Finland

www.eu-egee.org

Information Society and Media

Outline

- gJAF Overview
- Completion of the extension of the test suite
- Work on the new generic attributes voms PDP (Shibboleth inter-operability)
  - some problems
  - how to move forward
- Work plan & status

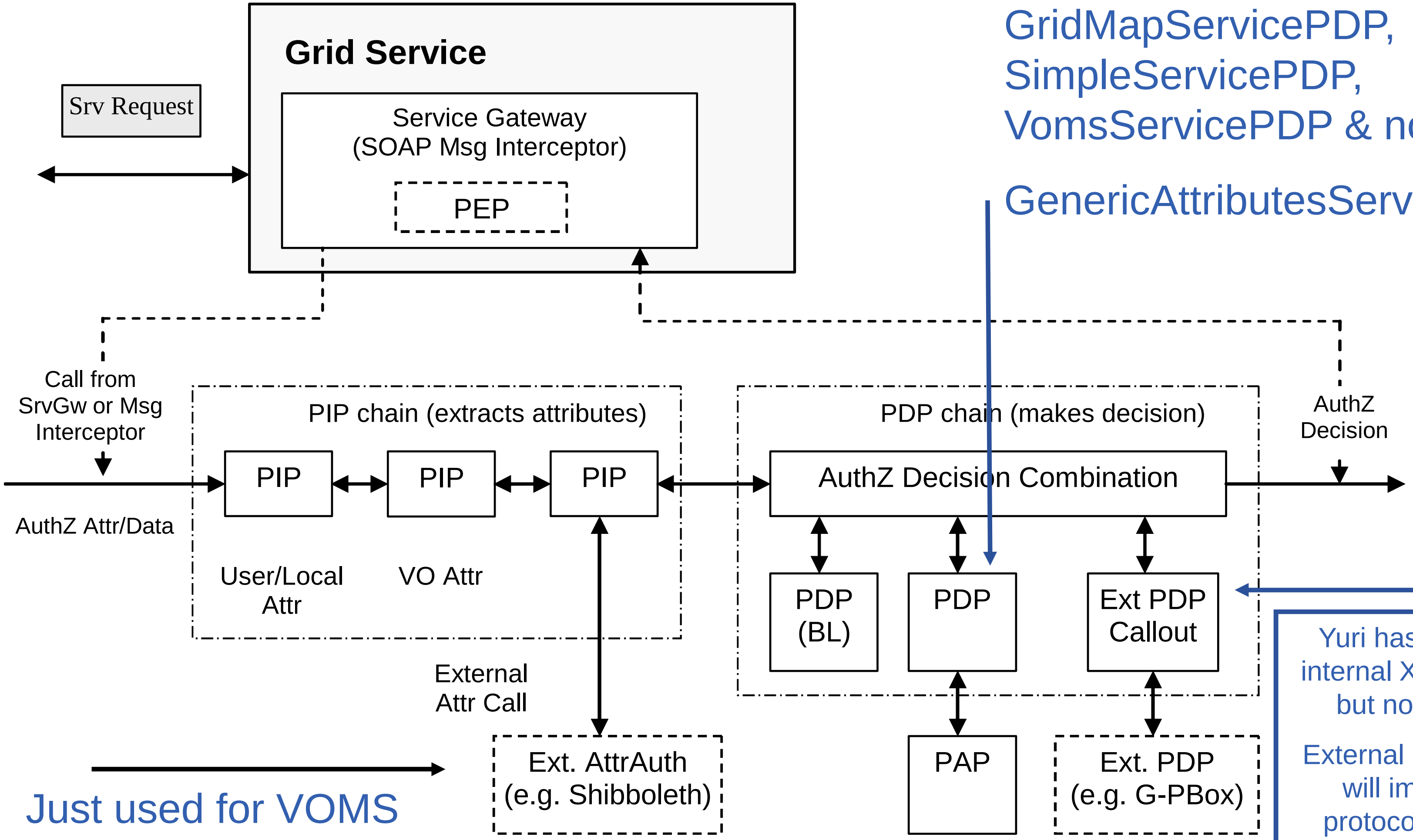
gJAF Overview (Briefly)

- **Provided as org.glite.security.authz Java package**
  - Uses actively java-utils library for VOMS

  (alternatively voms java api directly for voms libraries)
- **Called from applications via an interceptor (PEP)**
  - {MessageContext, Subject, operation}
- **Contains a configured chain of PIP and PDP modules**
  - PIP collects/extracts information to be sent to PDP
  - Each PDP evaluates its relevant attributes against its own Policy
  - Chain is configured to apply PDP decisions combination
- **Problems**
  - Requires application specific manual chain configuration
  - Limited use up to now in gLite
    - CE/CREAM

Enabling Grids for E-sciencE

gJAF components and connection to the Grid Service (Today)



GridMapServicePDP, SimpleServicePDP, VomsServicePDP & now

GenericAttributesServicePDP

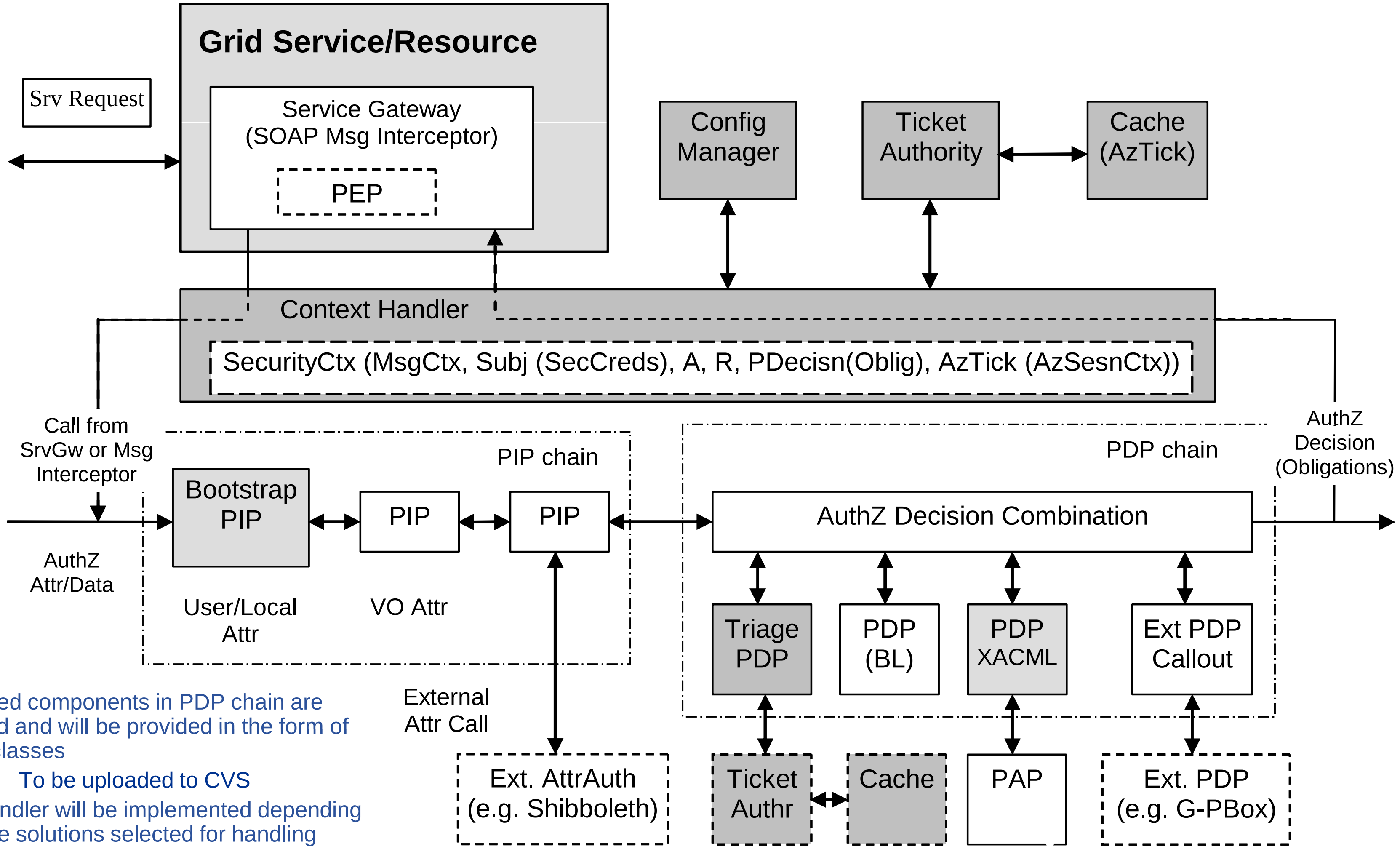
Just used for VOMS

attributes. Might need extension in Shibboleth phase III

Yuri has tested an internal XACML PDP but not in CVS.

External PDP callout will implement protocol currently being discussed between GT-OSG-EGEE

gJAF – Proposed Extensions



- All suggested components in PDP chain are tested and will be provided in the form of test classes
  - To be uploaded to CVS
- Context Handler will be implemented depending on the solutions selected for handling Obligations
  - Subject to GT-OSG-EGEE compatibility discussions

gJAF Extensions and GT-OSG-EGEE interoperability

- **gJAF extension is put into the context of GT-OSG-EGEE Site Central AuthZ Service (SCAzS) interoperability**
  - Most of suggested (earlier) extensions will depend on interoperability recommendations
  - ContextHandler will be implemented depending on the solutions selected for handling Obligations
    - Initially proposed to handle Obligations and AuthZ session
    - Currently suggested by GT-EGEE Obligations handling method by PEP at the time of receiving PDP response doesn't require introducing a ContextHandler
      - *However a problem of applying Obligations at later time of the resource access will remain*
- **Implementing SCAzS will require doing external PDP callout**
  - Presumably using GT-XACML PDP as a SCAzS
  - SAML2.0 profile of XACMLv2.0 is recommended as a protocol and an assertion format

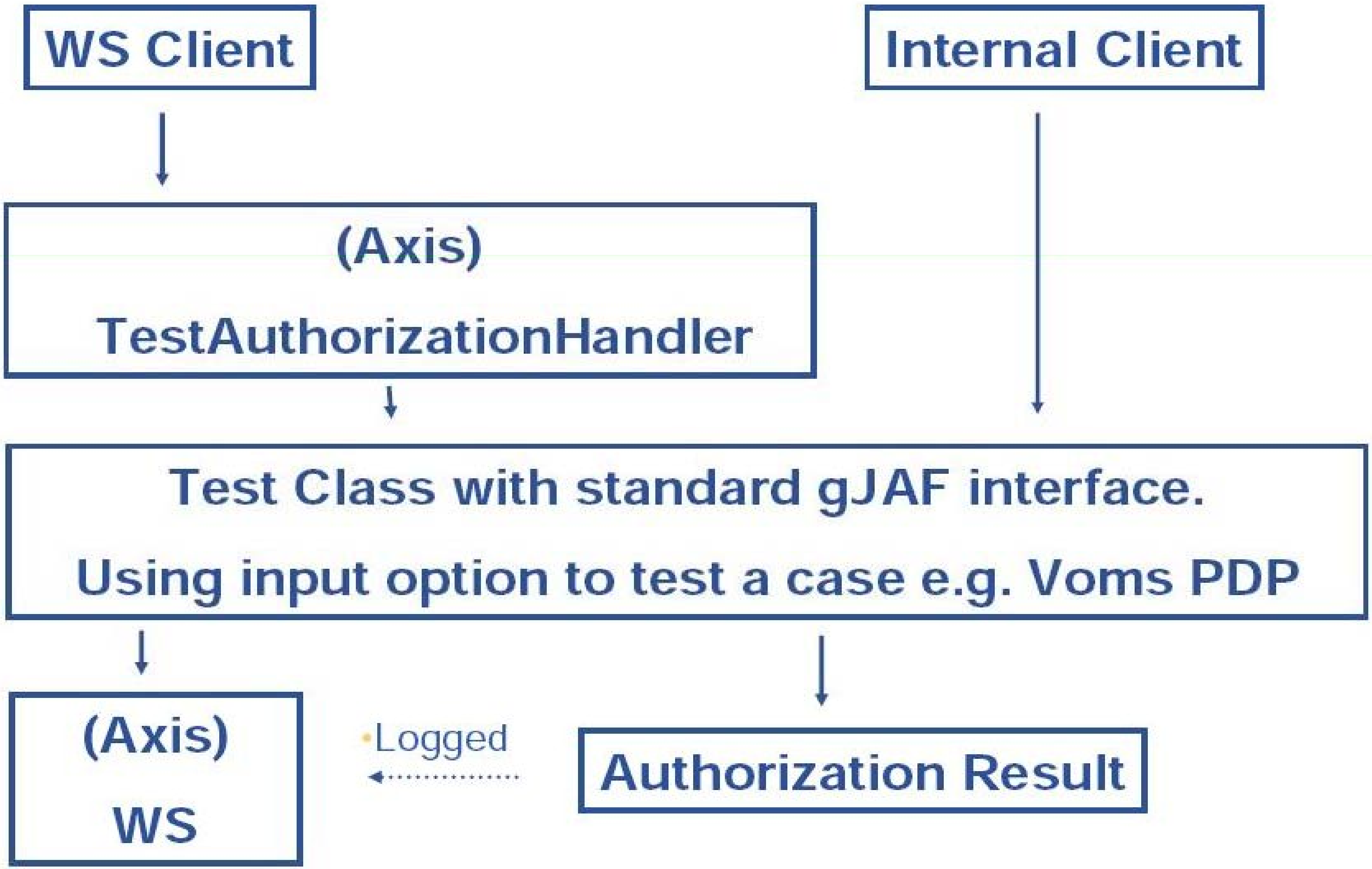
An extension of the test suite

- **Two types:**
  - junit test for e.g. test by building (existing)
  - Application use cases of gJAF (NEW!)

- **Why an extension?**
  - To promote gJAF to potential users
  - To help developers

- **Can test both the case of call from a web service and from a java internal client on the server side.**
  - A tutorial is added on cvs under org.glite.security.authz/test/conf

How does it work?



WS Client

Internal Client

(Axis)

TestAuthorizationHandler

Test Class with standard gJAF interface.

Using input option to test a case e.g. Voms PDP

(Axis)

WS

- Logged

Authorization Result

Generic attributes PDP

- A Generic attribute is an extension of voms to handle Name-value pairs which are used in the “Shibboleth world”.
- Generic attributes can be accessed through the VOMS API.
- In other words generic attributes can be treated very much the same way as in the VomsServicePDP, however, you have to compare extra generic attributes from a policy file with the ones in the voms proxy.

Problems

Needs:

- You need a relatively new version of VOMS (client and server)
- You need a Shibboleth account
- You need SLCS to create a x509 cert
- You need VASH to push your attributes on the VOMS

- SWITCH helped me with this

- At the moment we’re not able to rebuild the trust chain. Problems locally? Or bug? Vincenzo is on the case☺

- Open question: Use VomsPolicy class, or create a new one.

Work plan & status

- **SAML/Shib Credentials support**
  - Need to clarify SAML Assertions format and supporting libraries
    - To be provided as internal gJAF package or part of java-utils
  - Will rely on effective cooperation with SWITCH

  Status: Awaiting SWITCH phase III to discuss approach

- **Using XACML for policy expression**
  Motivation - Standard, Context aware, can be mapped to different formats
    - Used in G-PBox
  - Will be added as XACML PDP plugin to gJAF and as a callout to external PDP-XACML (e.g. implemented as Site Central AuthZ Service – currently discussed with GT-OSG)
  - Need policy management tool (simple or complex)

  Status:
  - All components are developed and tested locally but not committed to CVS
  - Callout interface will implement solution agreed between GT-OSG-EGEE

Work plan & status II

- **Other issues found important**
  - Handle XACML Policy Obligations
    - Will require either PDP chain to respond with Obligated decision or just using external callout to XACML based SCAzS
    - Initial implementation will depend on current discussion about Obligations handling standardisation between GT/OSG and gLite
  - PDP answer with AuthZ ticket to provide extended/full decision context in response to gJAF/PDP
    - Although all components are available at UvA this development and implementation is put behind joint GT-OSG-EGEE solution for Obligations

Status: Ongoing (in coordination with GT-OSG)

- **New issue discovered as a result of potential use/introduction of SCAzS**
  - Need to define and standardise site central Policy Repository Service (PRS) protocol
    - To be based on SAML2.0 profile of XACML that defines XACMLPolicy Query and Statement

Other issues?

- **New co-worker from 01.08**
  - Håkon Sagehaug (University of Bergen)
  - He will continue the work of UiB. Trygve will still be involved as contact person and attending conferences/meetings.

- **Other issues?**