gLite Java Authorisation Framework (gJAF) – Status and Development plans

Yuri Demchenko
University of Amsterdam
Trygve Aspelien
University of Bergen

EGEE2 JRA1 All-Hands meeting
March 7-9, 2007, Catania, Sicily

www.eu-egee.org

Information Society and Media

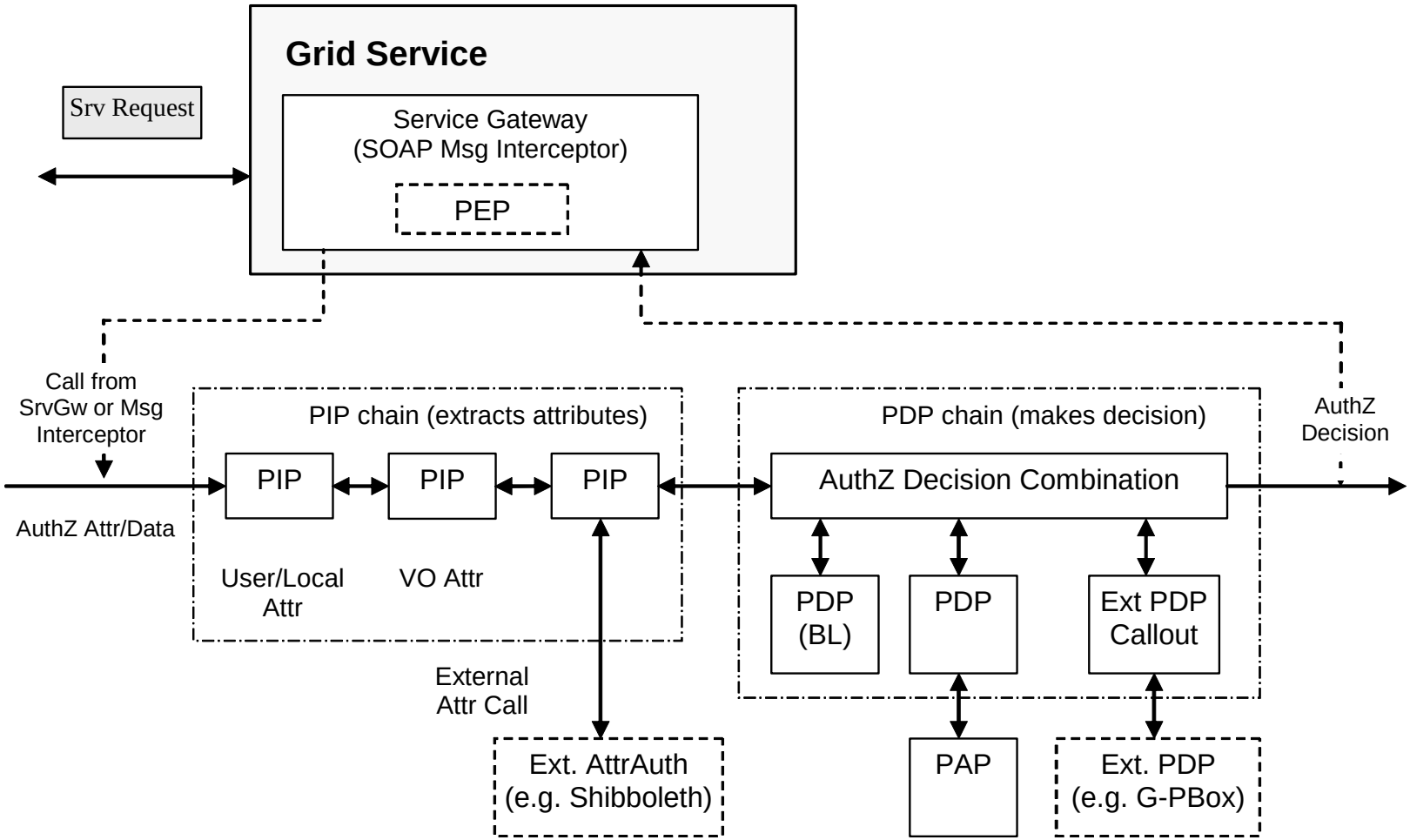
Outline

- **gJAF update and development**
  - Test setup for gJAF
  - Adding SAML and XACML support
- **Suggested further gJAF development/extensions**
  - Extended XACML support and AuthZ session support
- **Discussion**

gJAF Overview – Current Design

- **Provided as org.glite.security.authz Java package**
  - Uses actively org.glite.security.utils
  - Has inherited (architectural) compatibility with GT4-AuthZ
- **Called from applications via an interceptor/gateway**
  - {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 by CREAM
    - AuthZ functionality is dispersed between gJAF and CREAM components

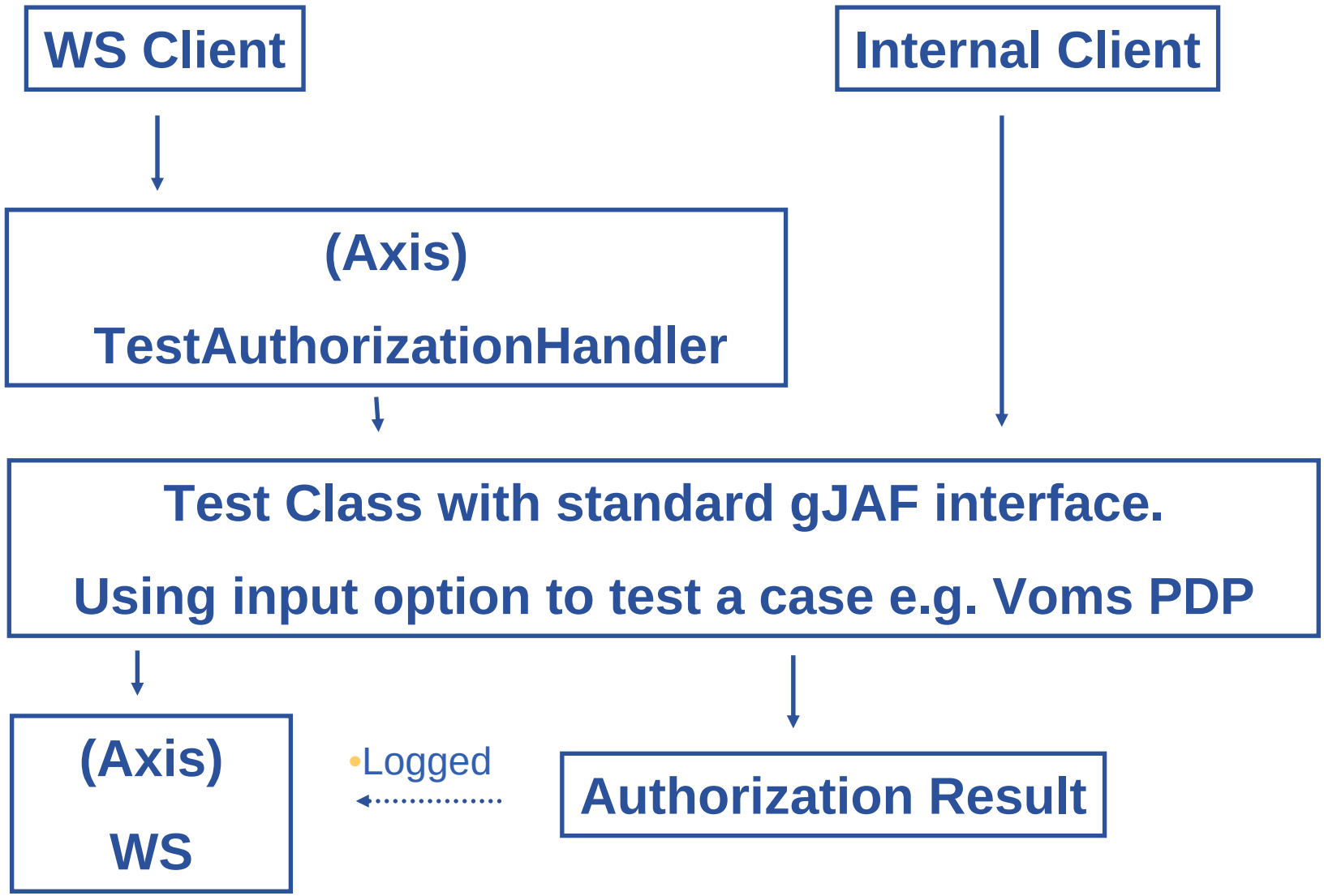
gJAF components and connection to the Grid Service (current design)



gJAF Overview – Current works

- **Fixing bugs (past and recent)**
  - Bug #18244 and #21544 fixed so far (with significant help from CREAM group)
  - New bug assigned - #????
- **Creating test suite/installation to assist gJAF development and maintenance (work done by Trygve Aspelien, UiB)**
  - Currently gJAF lacks testing environment for developers for bug fixing and general testing
    - The documentation is very general and limited with examples
  - Will help gJAF promotion to other EGEE activities and potentially external projects
  - gJAF can be used with Web Services (WS) or as an internal gLite java client on the server side

Test suite gJAF structure (Working)

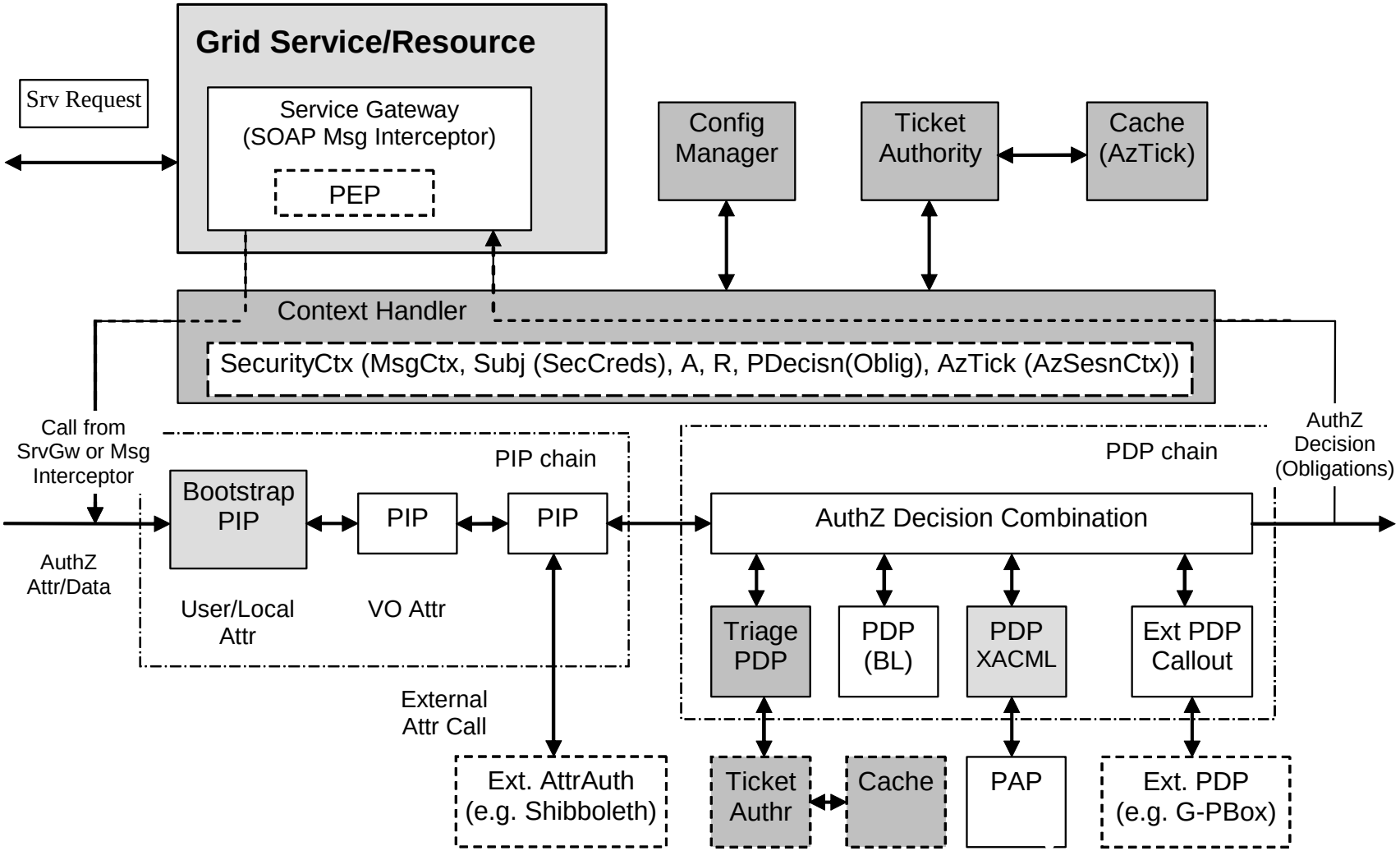


Test suite gJAF WS/Internal

What to do and status:

- Writing a tutorial (In progress)
- Create a WS environment [wsdl file, service and client] (Done)
- Create an internal client (Done)
- Create a simple blacklist PDP test case (Done)
- Create a voms PDP test case (In planning/progress)
- Policy file format and handling (Discussion/planning)
- Later: Other PDP's, (e.g., for Shibboleth)

gJAF – Proposed Extensions



gJAF extensions (1) – SAML and Shibboleth attributes

- **Shibboleth-VOMS attributes support for AuthZ**
  - Regular discussion with SWITCH team started
  - Current stage 2 doesn't require SAML support but implemented via VOMS-shibboleth interaction
- **Adding SAML based credentials support both generic and for later stages of Shibboleth integration**
  - To be provided as internal gJAF package or part of org.glite.security.utils and supported by SAML PIP
- **Issues for discussion**
  - Configuring key/certificates used in validation of SAML Attribute and Authorisation assertions
  - May need (site) AuthZ service key to sign AuthZ assertion/ticket
    - Host key can be used in general

gJAF extensions (2) – XACML policy support

- **Goal: To have the same functionality as LCAS/LCMAPS (which provides also account mapping)**
  - Can be solved with XACML Obligations support
- **Simple internal XACML PDP and external PDP callouts to e.g. G-PBox**
  - Needs XACML policy editor/generation tool (simple or complex)
- **XACML related issues that require gJAF re-design**
  - Enable PDP chain to respond with Obligated decision
    - Needed to provide account mapping
  - PDP/gJAF response with AuthZ Assertion/ticket to provide extended AuthZ decision context
    - *SAML and proprietary AuthZ assertions*
    - Potentially can support ***AuthZ session management***

Further proposed developments

- **Compatibility and integration with other gLite/EGEE and 3rd party solutions**
  - Integration with the G-PBox
    - Needs gJAF AuthZ chain extension to process Obligated decisions
  - Compatibility and integration with the GT4-AuthZ
    - Possibility to reuse available set of PDP's and PIP's
    - Interest in cooperate and compatibility from the GT4-AuthZ team
- **Minimum common XACML Policy profile**
  - Policy formats mapping – XACML, GACL, ACL, gridmap, BlackList
    - Q: Are all they compatible and convertible (e.g. to XACML)?
- **Authorisation session support**
  - AuthZ session assertion/ticket (details in appendix)

Other related activities

- **gJAF documentation update**
  - Time to update gJAF Developer's guide - https://edms.cern.ch/document/501718
    - Will be especially needed for adding Shibboleth SAML Attributes assertions support and wider SAML assertions support
  - HOWTO and usage examples
- **EGEE AuthZ Policy Coordination**
  - 2 face-to-face meetings
    - EGEE2 in Bologna on January 18-19, 2007
    - EGEE1 in Bologna on June 6-7, 2005
  - *Outcome of the last meeting*
    - (1) practical/technical suggestions for further gJAF development
    - *(2) suggestions for coordination with other EGEE activities and external projects*
    - *(3) pushing EGEE AuthZ experience through OGF OGSA- AuthZ WG*
      - *Bring EGEE reality to OGF standardisation*

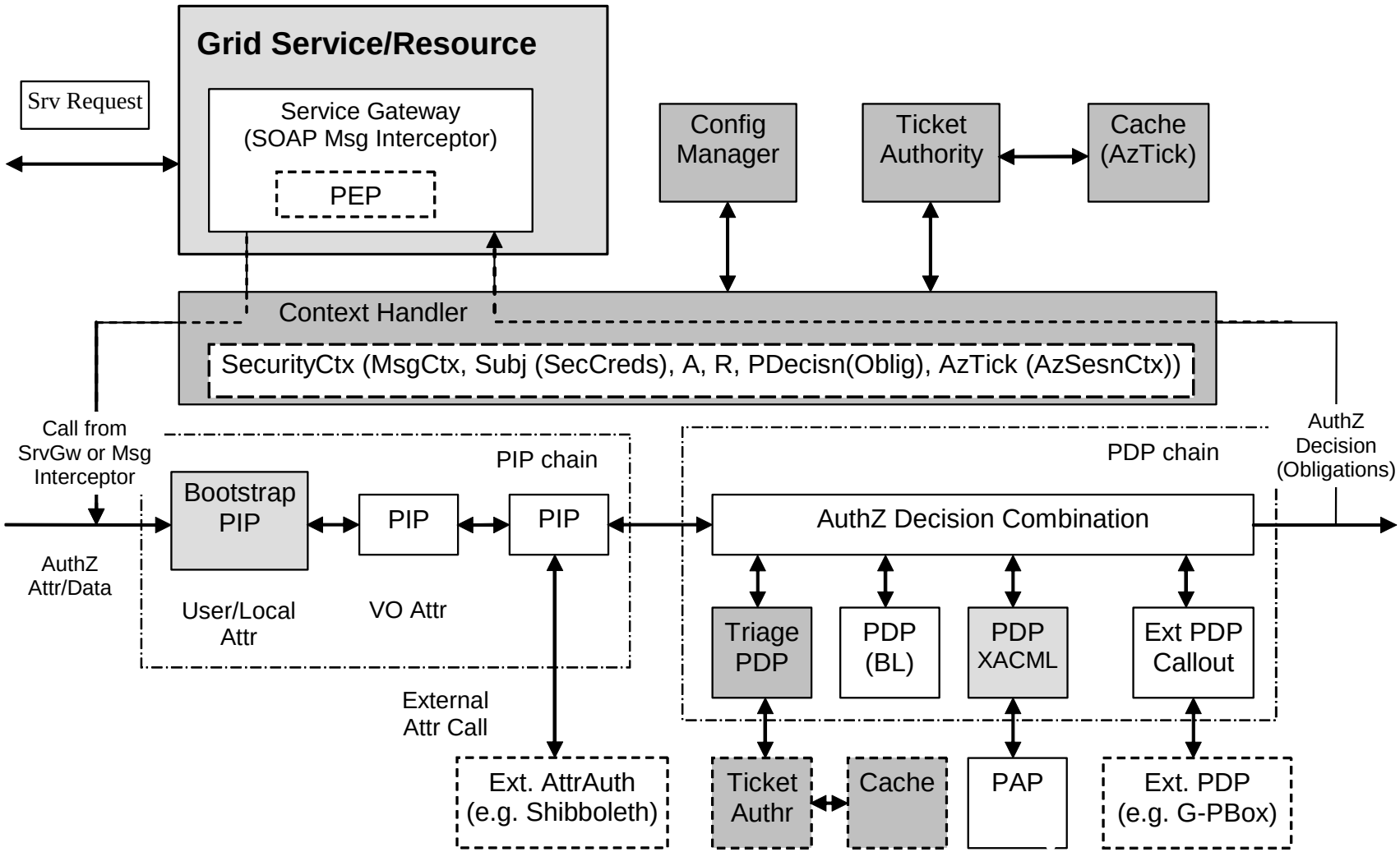
Discussion

- Common XACML policy format
- AuthZ Session support and AuthZ Ticket format
- Any other issues?

Additional information

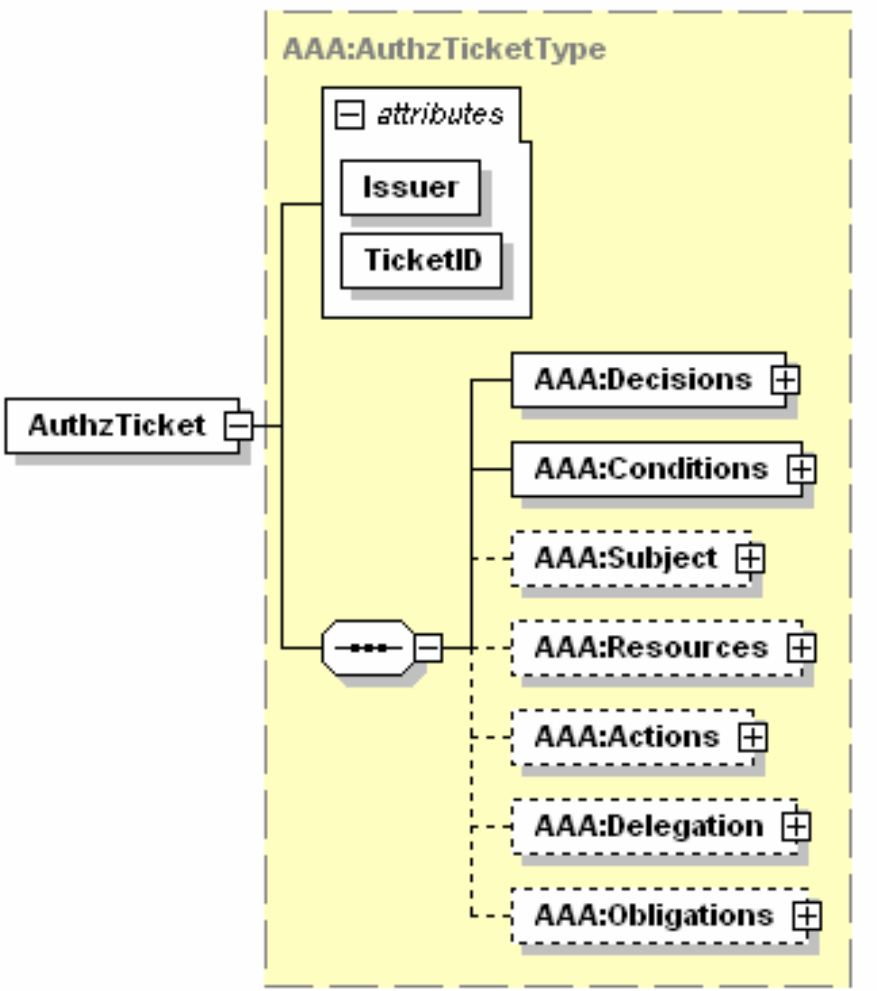
- **AuthZ Ticket format (details)**
- **GT4 Authorisation Framework**

gJAF – Proposed Extensions



AuthZ session management and AuthZ ticket format

AuthZ ticket - Top elements



AuthZ ticket is a way to support AuthZ session

- Required for central site AuthZ service
- Provides flexibility in resource allocation and access control management

AuthZ ticket - Top elements

- **<Decisions>/<Decision> - hold the PDP AuthZ decision bound to the requested resource or service expressed as the ResourceID attribute and related {S, R, A}**
- **<Conditions> - specifies the validity constrains for the ticket, including validity time and AuthZ session identification and additionally context**
  - <ConditionAuthzSession> (extendable) - holds AuthZ session context
- **<Subject> complex element - contains all information related to the authenticated Subject who obtained permission to do the actions**
  - <Role> - holds subject's capbilities
  - <SubjectConfirmationData> - typically holds AuthN context
  - <SubjectContext> (extendable) - provides additional security or session related information, e.g. Subject's VO, project, or federation.
- **<Resources>/<Resource> - contains resources list access to which is granted by the ticket**
- **<Actions>/<Action> complex element - contains actions which are permitted for the Subject or its delegates**
- **<Delegation> element – defines who the permission and/or capability are delegated to: another Subjects or community**
  - attributes define restriction on type and depth of delegation
- **<Obligations>/<Obligation> - holds obligations that PEP/Resource should perform in conjunction with the current PDP decision.**

AuthZ ticket – Example Version 0.0 (proprietary format)

```
<AAA:AuthzTicket xmlns:AAA="http://www.aaauthreach.org/ns/#AAA" Issuer="urn:cnl:trust:tickauth:pep"
    TicketID="cba06d1a9df148cf4200ef8f3e4fd2b3">
  <AAA:Decision ResourceID="http://resources.collaboratory.nl/Philips_XPS1">Permit</AAA:Decision>
    <!-- SAML mapping: <AuthorizationDecisionStatement Decision="*" Resource="*"> -->
  <AAA:Actions>
    <AAA:Action>cnl:actions:CtrlInstr</AAA:Action>     <!-- SAML mapping: <Action> -->
    <AAA:Action>cnl:actions:CtrlExper</AAA:Action>
  </AAA:Actions>
  <AAA:Subject Id="subject">
    <AAA:SubjectID>WHO740@users.collaboratory.nl</AAA:SubjectID> <!-- SAML mapping:<Subject>/<NameIdentifier> -->
    <AAA:SubjectConfirmationData>IGhA11vwa8YQomTgB9Ege9JRNnld84AggaDkOb5WW4U=</AAA:SubjectConfirmationData>
    <!-- SAML mapping:  EXTENDED <SubjectConfirmationData/> -->
    <AAA:Role>analyst</AAA:Role>
    <!-- SAML mapping:  <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue> -->
    <AAA:SubjectContext>CNL2-XPS1-2005-02-02</AAA:SubjectContext>
    <!-- SAML mapping: <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue> -->
  </AAA:Subject>
  <AAA:Delegation MaxDelegationDepth="3" restriction="subjects">
    <!-- SAML mapping:  LIMITED <AudienceRestrictionCondition> (SAML1.1), or <ProxyRestriction>/<Audience>
    (SAML2.0)  -->
    <AAA:DelegationSubjects> <AAA:SubjectID>team-member-2</AAA:SubjectID> </AAA:DelegationSubjects>
  </AAA:Delegation>
  <AAA:Conditions NotBefore="2006-06-08T12:59:29.912Z" NotOnOrAfter="2006-06-09T12:59:29.912Z" renewal="no">
    <!-- SAML mapping: <Conditions NotBefore="*" NotOnOrAfter="*"> -->
    <AAA:ConditionAuthzSession PolicyRef="PolicyRef-GAAA-RBAC-test001" SessionID="JobXPS1-2006-001">
    <!-- SAML mapping: EXTENDED <SAMLConditionAuthzSession PolicyRef="*" SessionID="*"> -->
      <AAA:SessionData>put-session-data-Ctx-here</AAA:SessionData>  <!-- SAML EXTENDED: <SessionData/> -->
    </AAA:ConditionAuthzSession>
  </AAA:Conditions>
  <AAA:Obligations>
    <AAA:Obligation>put-policy-obligation(2)-here</AAA:Obligation>  <!-- SAML EXTENDED:
    <Advice>/<PolicyObligation> -->
    <AAA:Obligation>put-policy-obligation(1)-here</AAA:Obligation>
  </AAA:Obligations>
</AAA:AuthzTicket>
<ds:Signature> <ds:SignedInfo/>
    <ds:SignatureValue>e4E27kNwEXoVdnXIBpGVjpaBGVY71Nypos...</ds:SignatureValue></ds:Signature>
```

AuthZ ticket - Top elements (2)

- **<Decisions>/<Decision> - hold the PDP AuthZ decision bound to the requested resource or service expressed as the ResourceID attribute and related {S, R, A}**
- **<Conditions> - specifies the validity constrains for the ticket, including validity time and AuthZ session identification and additionally context**
  - <ConditionAuthzSession> (extendable) - holds AuthZ session context
- **<Subject> complex element - contains all information related to the authenticated Subject who obtained permission to do the actions**
  - <Role> - holds subject's capbilities
  - <SubjectConfirmationData> - typically holds AuthN context
  - <SubjectContext> (extendable) - provides additional security or session related information, e.g. Subject's VO, project, or federation.
- **<Resources>/<Resource> - contains resources list access to which is granted by the ticket**
- **<Actions>/<Action> complex element - contains actions which are permitted for the Subject or its delegates**
- **<Delegation> element – defines who the permission and/or capability are delegated to: another Subjects or community**
  - attributes define restriction on type and depth of delegation
- **<Obligations>/<Obligation> - holds obligations that PEP/Resource should perform in conjunction with the current PDP decision.**

AuthZ ticket – Example Version 0.0 (proprietary format)

```
<AAA:AuthzTicket xmlns:AAA="http://www.aaauthreach.org/ns/#AAA" Issuer="urn:cnl:trust:tickauth:pep"
    TicketID="cba06d1a9df148cf4200ef8f3e4fd2b3">
  <AAA:Decision ResourceID="http://resources.collaboratory.nl/Philips_XPS1">Permit</AAA:Decision>
    <!-- SAML mapping: <AuthorizationDecisionStatement Decision="*" Resource="*"> -->
  <AAA:Actions>
    <AAA:Action>cnl:actions:CtrlInstr</AAA:Action>     <!-- SAML mapping: <Action> -->
    <AAA:Action>cnl:actions:CtrlExper</AAA:Action>
  </AAA:Actions>
  <AAA:Subject Id="subject">
    <AAA:SubjectID>WHO740@users.collaboratory.nl</AAA:SubjectID> <!-- SAML mapping:<Subject>/<NameIdentifier> -->
    <AAA:SubjectConfirmationData>IGhA11vwa8YQomTgB9Ege9JRNnld84AggaDkOb5WW4U=</AAA:SubjectConfirmationData>
    <!-- SAML mapping:  EXTENDED <SubjectConfirmationData/> -->
    <AAA:Role>analyst</AAA:Role>
    <!-- SAML mapping:  <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue> -->
    <AAA:SubjectContext>CNL2-XPS1-2005-02-02</AAA:SubjectContext>
    <!-- SAML mapping: <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue> -->
  </AAA:Subject>
  <AAA:Delegation MaxDelegationDepth="3" restriction="subjects">
    <!-- SAML mapping:  LIMITED <AudienceRestrictionCondition> (SAML1.1), or <ProxyRestriction>/<Audience>
    (SAML2.0)  -->
    <AAA:DelegationSubjects> <AAA:SubjectID>team-member-2</AAA:SubjectID> </AAA:DelegationSubjects>
  </AAA:Delegation>
  <AAA:Conditions NotBefore="2006-06-08T12:59:29.912Z" NotOnOrAfter="2006-06-09T12:59:29.912Z" renewal="no">
    <!-- SAML mapping: <Conditions NotBefore="*" NotOnOrAfter="*"> -->
    <AAA:ConditionAuthzSession PolicyRef="PolicyRef-GAAA-RBAC-test001" SessionID="JobXPS1-2006-001">
    <!-- SAML mapping: EXTENDED <SAMLConditionAuthzSession PolicyRef="*" SessionID="*"> -->
      <AAA:SessionData>put-session-data-Ctx-here</AAA:SessionData>  <!-- SAML EXTENDED: <SessionData/> -->
    </AAA:ConditionAuthzSession>
  </AAA:Conditions>
  <AAA:Obligations>
    <AAA:Obligation>put-policy-obligation(2)-here</AAA:Obligation>  <!-- SAML EXTENDED:
    <Advice>/<PolicyObligation> -->
    <AAA:Obligation>put-policy-obligation(1)-here</AAA:Obligation>
  </AAA:Obligations>
</AAA:AuthzTicket>
<ds:Signature> <ds:SignedInfo/>
    <ds:SignatureValue>e4E27kNwEXoVdnXIBpGVjpaBGVY71Nypos...</ds:SignatureValue></ds:Signature>
```

AuthzToken example – 293 bytes

```
<AAA:AuthzToken TokenID="c24d2c7dba476041b7853e63689193ad">
<AAA:TokenValue>
0IZt9WsJT6an+tIxhhTPtiztDpZ+iynx7K7X2Cxd2iBwCUTQ0n61Szv81DKllWsq75IsHfusnm56
zT3fhKU1zEUsob7p6oMLM7hb42+vjfvNeJu2roknhIDzruMrr6hMDsIfaotURepu7QCT0sADm9If
X89Et55EkSE9oE9qBD8=
</AAA:TokenValue>
</AAA:AuthzToken>
```

AuthzToken is constructed of the AuthzTicket TicketID and SignatureValue

AuthzToken use suggests caching AuthzTicket's

GT4 Authorisation Framework

- **Can be configured for Container, Message, Service/Resource**
  - Called from the SOAP/Axis message interceptor
- **AuthZ processing sequence includes**
  - Bootstrapping X.509 PIP – retrieves request parameters from the message
    - Subject, Resource, Action
  - Sequence of pre-configured PIP's, including SAML
  - Sequence of (specialised) PDP's
  - Different PDP decisions combination algorithms by AuthZ engine
    - However, multiple policy decision's consistency is not resolved
- **Available PDP's**
  - ACL and GridMap
  - HostAuthorization and UserNameAuthorization (similar BlackList PDP)
  - SAML AuthZ callout and SAML AuthZ Assertion
  - SelfAuthorization – based on shared/trusted Resource credentials
  - Simple XACML PDP (provided as a placeholder for extension)

AuthZ Coordination Initiatives

- **OGSA-AUTHZ (**https://forge.gridforum.org/projects/ogsa-authz**) and other (OGF) initiatives**
  - Functional Components of Grid Service Provider Authorisation Service Middleware
  - Credential Validation Service (CVS)
    - Implements one of mechanism for interoperability
  - WS-TRUST and SAML to access a CVS and Request Context to access a PDP
  - CVS Requirements – not formal
- **Interoperation and integration with campuses**
  - Accepting Shibboleth attributes
    - VOMS-Shibboleth integration – GridShib, GridAAI (by SWITCH)