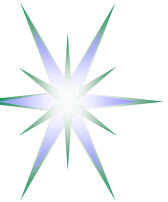
Using Workflow for Dynamic Security Context Management in Grid-based Application

Yuri Demchenko <demch@science.uva.nl>
System and Network Engineering Group
University of Amsterdam

Grid 2006 Conference
28-29 September 2006, Barcelona



Outline

- Goal and Background information
  - Basic use cases and target projects
- AuthZ service operation in Grid/WS based applications
  - Requirements and mechanisms to support dynamic security context
- GAAA-RBAC profile – design and implementation suggestions
  - Configuration and trust domains management
  - Extended AuthZ session management
- Summary – Future development
- Additional materials (technical)
  - Role Based Access Control (RBAC) and XACML policy examples
  - Using VO for dynamic security context management

GAAA – Generic Authentication, Authorization, Accounting

GAAA-AuthZ – GAAA AuthZ Framework

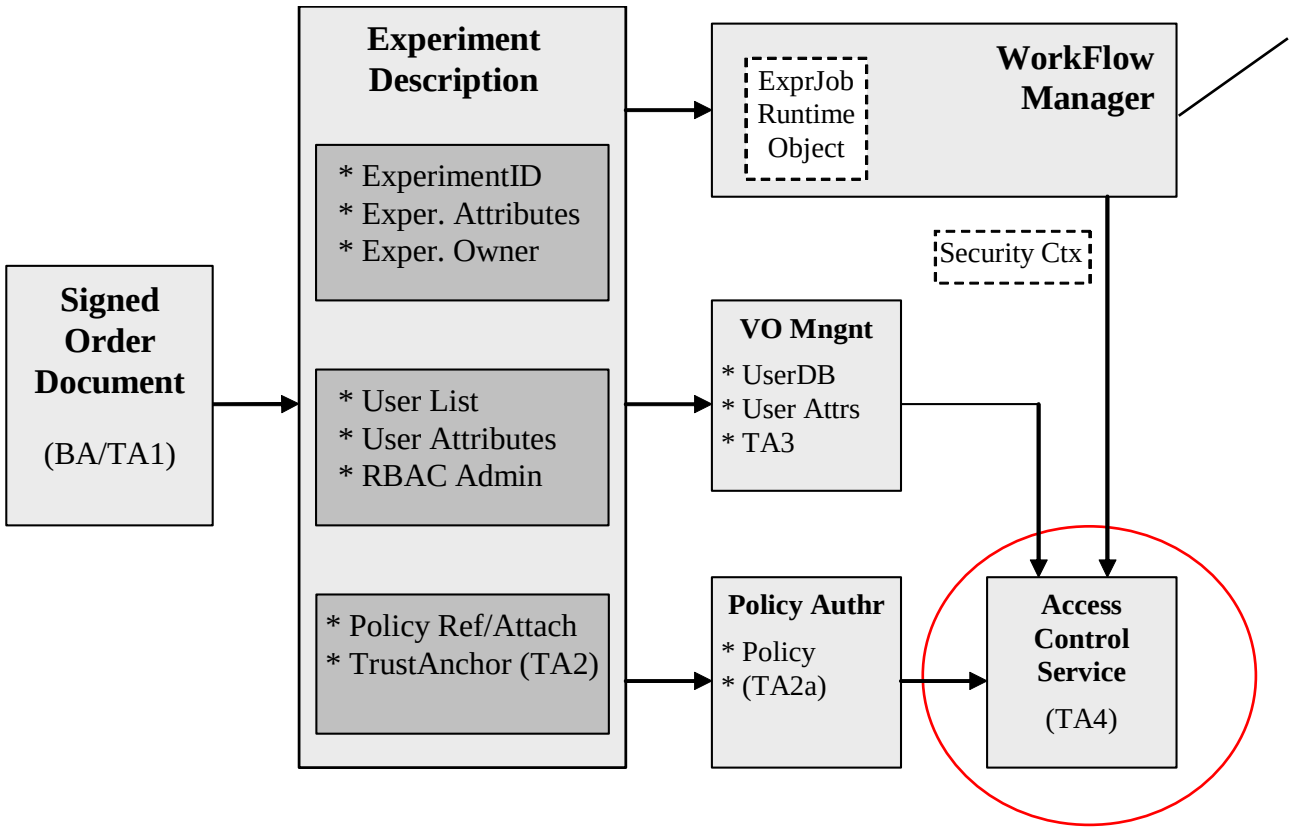
The goal of this research

- General - Add security features to the workflow and workflow management systems (WFMS)
- Stage 1 – Design approach to the Authorisation service that can be integrated with WFMS
- Stage 2 – Extensions to BPEL for business and scientific applications and/or a kind of “micro” workflow for handling complex AAA/AuthZ operations

Background – basic use cases and target projects

- Central Authorisation service for Grid based Collaborative applications
  - Architecture, Framework and Implementation (Collaboratory.nl project)
  - Implements Domain based resource management and RBAC (RBAC-DM)
  - Uses workflow based Experiment management
- Distributed multidomain Authorisation service for OLPP
  - NL national project RoN GP-NG and EU Project PHOSPHORUS
  - Requires extended AuthZ/provisioning session context management in multidomain scenario
  - AuthZ technology Gap analysis report is available
- AuthZ service for dynamic Grid applications
  - Development in the framework of the EGEE project and GT4-AuthZ team cooperation
  - gLite-AuthZ framework integration with the GT4-AuthZ
  - Extension for complex policy decisions and AuthZ session context management

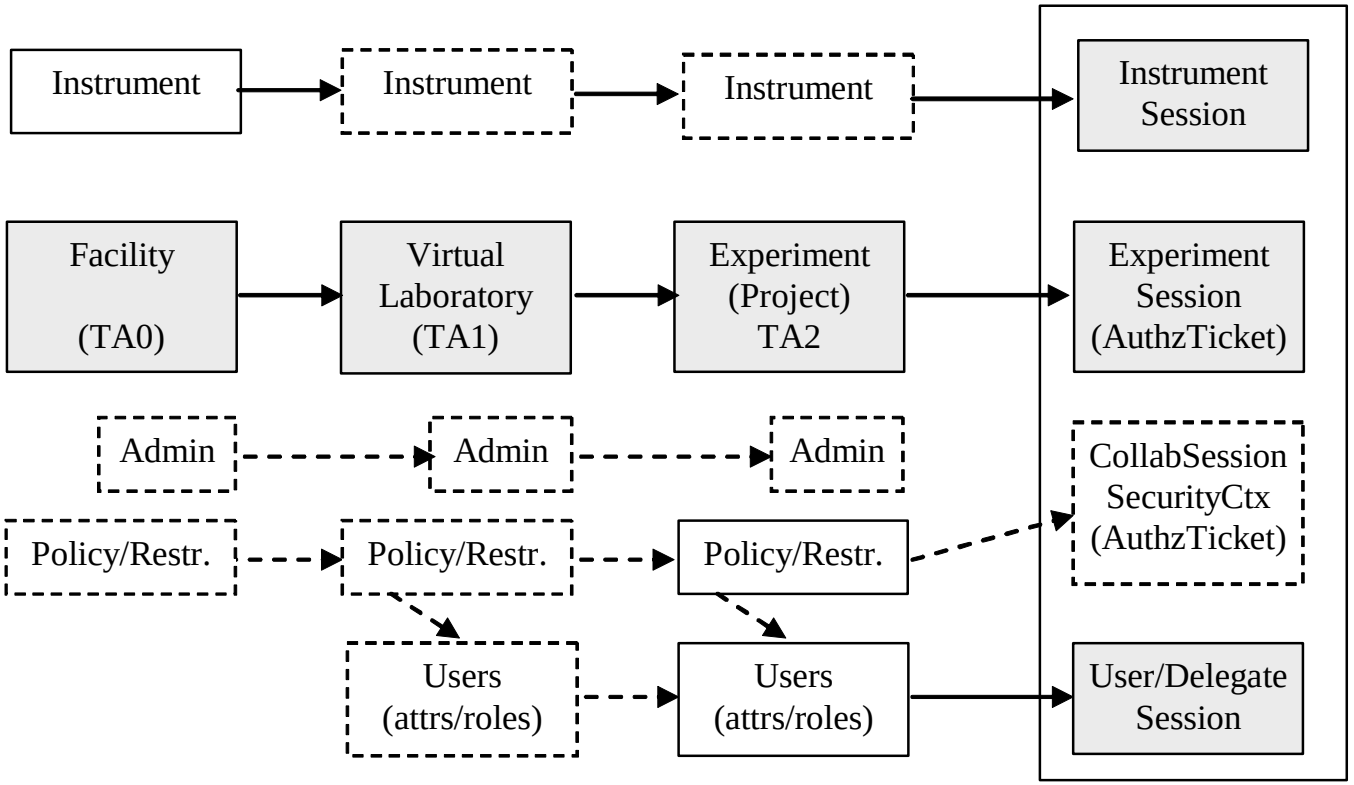
Experiment-centric security model using workflow for security context management (CNL project)



Experiment Description as a semantic object defining attributes for the workflow/job, user association in a form of VO, access control policy

Trust domain based on Business Agreement (BA) or Trust Anchor (TA)

Domain based Resource management



- Implements RBAC3 model + Experiment AuthZ session management
- Uses XACML RBAC profile and XACML v3.0 administrative policy profile

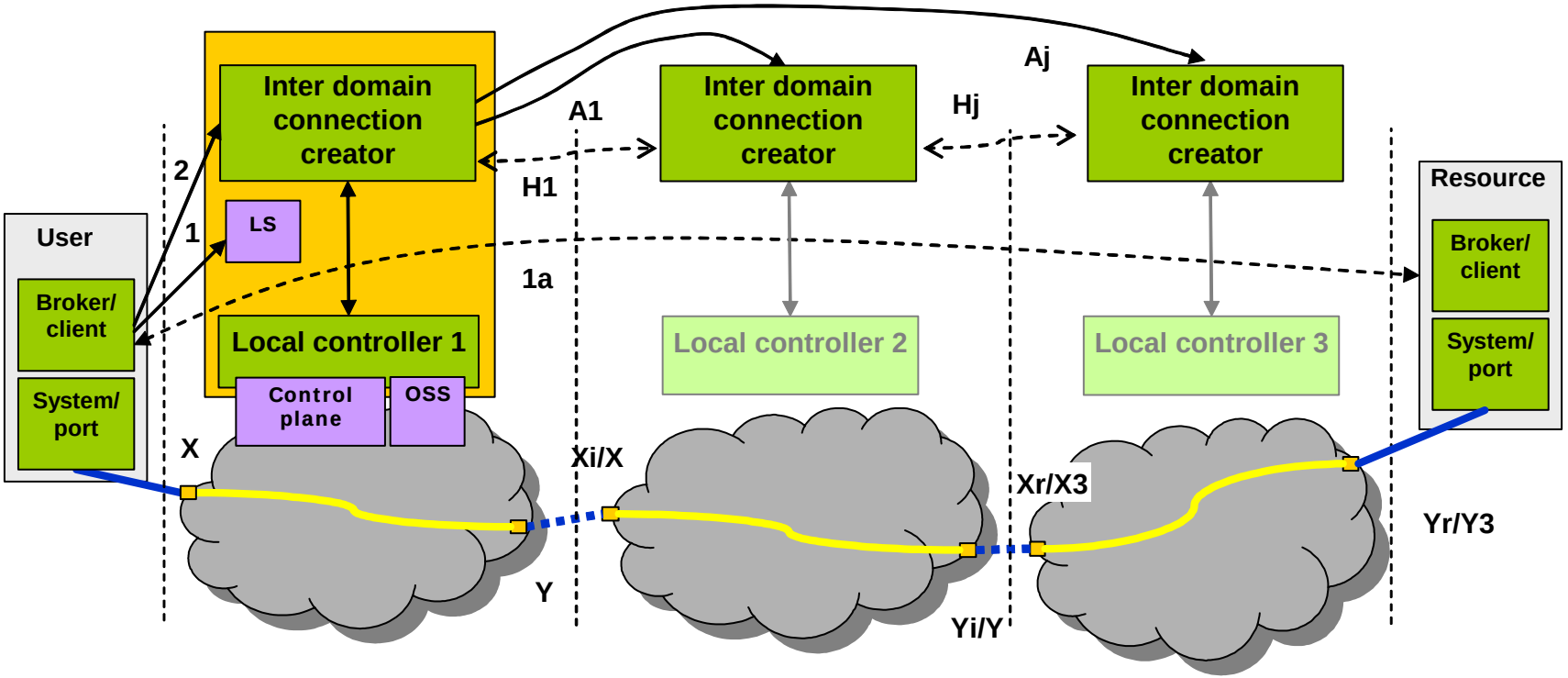
Full Resource URI/ID –

CNL:Facility:VirtualLab:Experiment:InstrModel

Full User Session context –

Facility < Virtual Lab < Experiment < Experiment Session < Collaborative Session

Multidomain Optical LightPath Provisioning (OLPP)



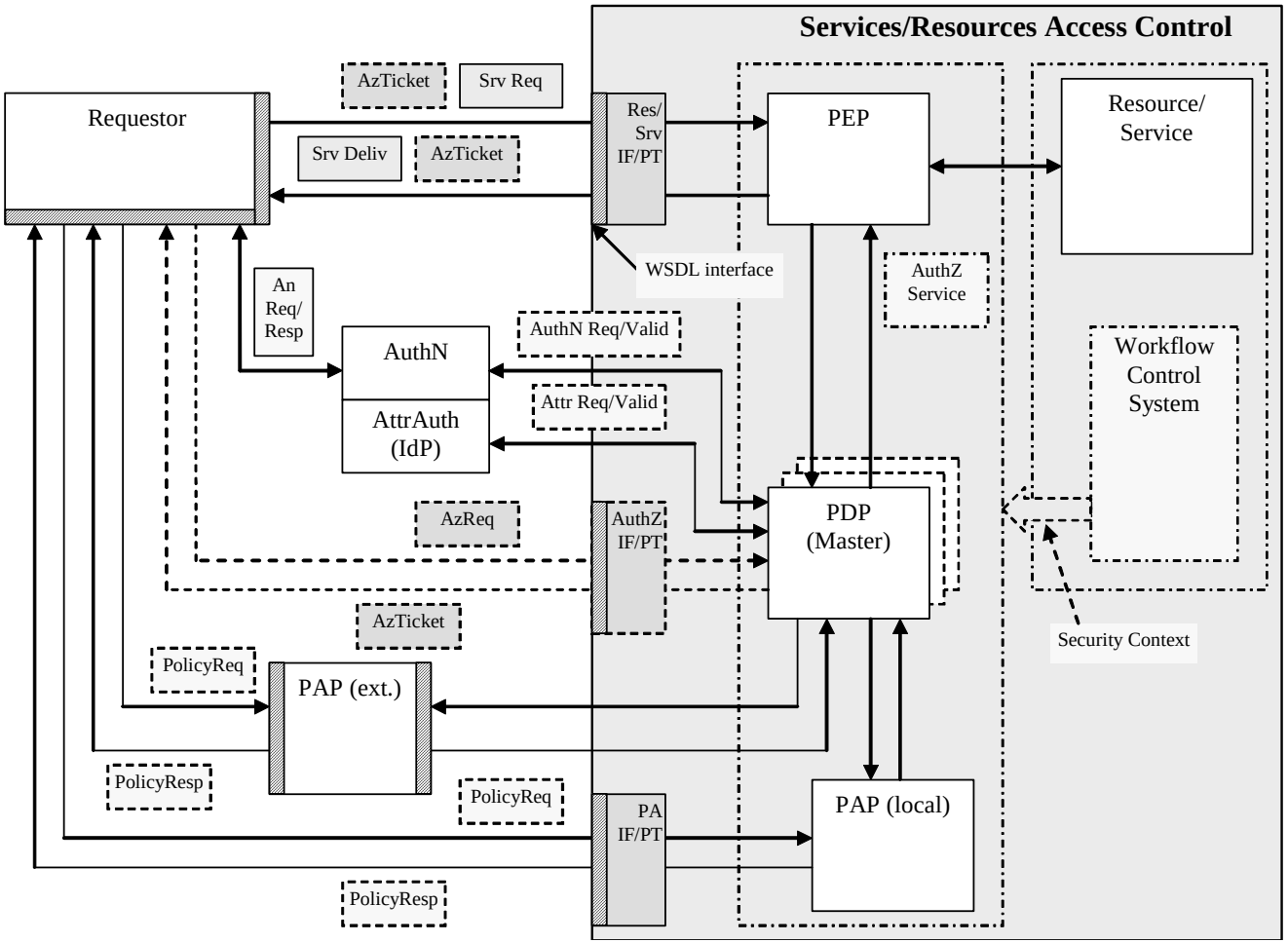
Major steps in complex resource provisioning

- Lookup/discovery
- Complex resource composition
- Reservation (secured by the Reservation ticket)
- Actual provisioning or delivery

Two basic operational modes

- (1) “hop-by-hop” and (2) agent based
- Both require handling multidomain policy, trust, and attribute semantics
- (1) requires full security Ctx exchange

AuthZ service operation in Grid/WS based applications



Security/Access control services integrated with the Workflow via Web Services ports and messages defintion

Message-level Security services are linked to SOAP header

Linking dynamically all components of the access control system

Policy is attached to any component of the service description in WSDL format

Interacting services will fetch policy document and apply restrictions/rules to elements, which declared policy compliance requirements

Security context management: Context dependent information and existing mechanisms

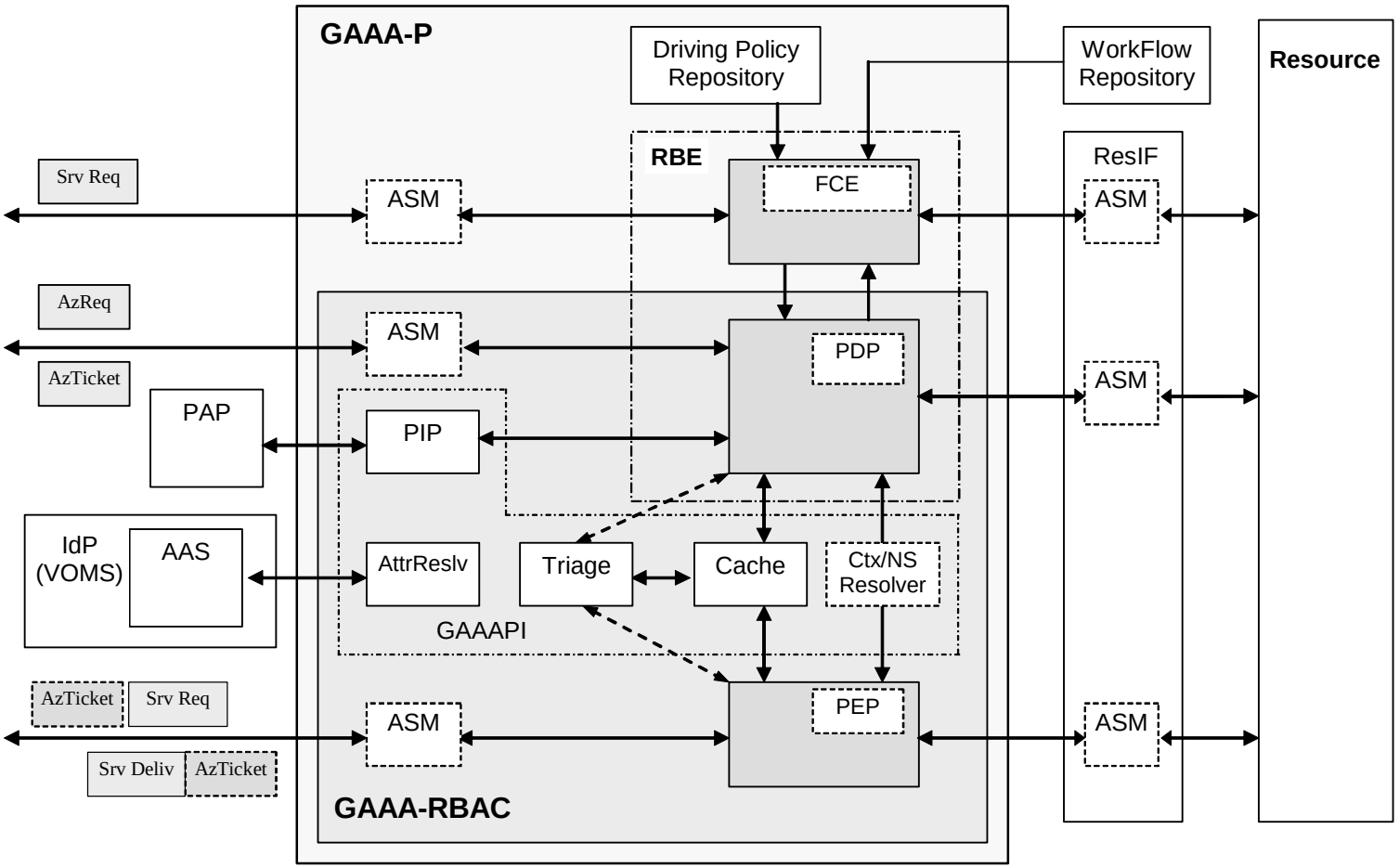
Context dependent information/attributes:

- Policy
- Trust domains and authorities
- Attributes namespaces
- Service/Resource environment/domain
- Credential semantics and formats

Mechanisms to transfer/manage context related information

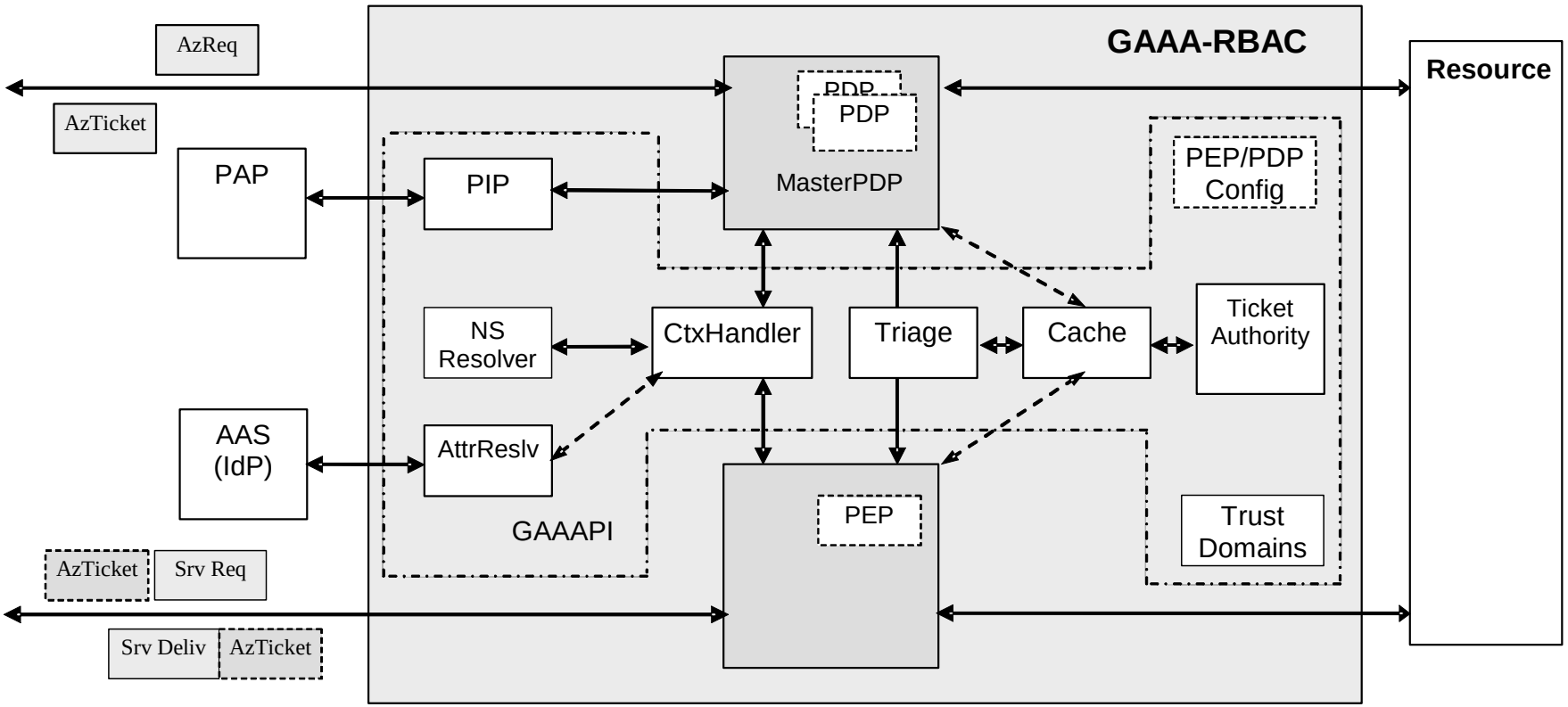
- Service and requestor/user ID/DN format that should allow for both using namespaces and context aware names semantics
- Attribute format (either X.509/X.521 or URN/SAML2.0 presentation)
- Context aware XACML policy definition using the Environment element of the policy Target element
- Security tickets and tokens used for AuthZ session management and for provisioned resource/service identification
- Security federations for users and resources, e.g. VO membership credentials

GAAA_tk profiles: GAAA-RBAC and GAAA-P



- **Profiles GAAA-P and GAAA-RBAC**
- **Trust domains and Authorities configuration**
- **AuthZ Session management**
- **AuthZ ticket and token format**
- **GT4/gLite integration**

GAAAPI components to support dynamic security context management (1)



- GAAAPI is a collection of components to support PEP and PDP interaction, implemented in Java supporting both GAAA-P and GAAA-RBAC profiles

GAAPI components to support dynamic security context management (2)

- Context Handler (CtxHandler) that calls to a namespace resolver (NS Resolver) and attribute resolver (AttrResolver), which in its own can call to external Attribute Authority Service (AAS) to validate presented attributes or obtain new ones
- Triage and Cache to provide an initial evaluation of the request, including the validity of the provided credentials
  - Used for handling AuthZ tickets/tokens, and also for AuthZ session management by evaluating service requests versus the provided AuthZ ticket/token claims
- Ticket Authority (TickAuth) generates and validates AuthZ tickets or tokens on request from PEP or PDP
  - to support AuthZ session, tickets are cached by TickAuth directly or by PEP/PDP
- Policy Information Point (PIP) that provides resolution and call-outs to related authoritative Policy Authority Points (PAP)

GAAA-RBAC/GAAAPI Security Configuration

General security configuration

- Key store location and access
- Trusted and local keys/credentials

Trust domains and authorities (depending on possible PEP and PDP location)

- PEP is protecting Resource, and therefore should be located in the Resource trust domain
- PDP may be remote, in this case communication between PEP and PDP must be protected cryptographically

PEP and PDP Configuration (at invocation time)

- Namespace Resolver
- AuthzTicket Authority (tickauthPDP | tickauthPEP)
- Trust domains
- Session credentials or AUthZ ticket/tokens format

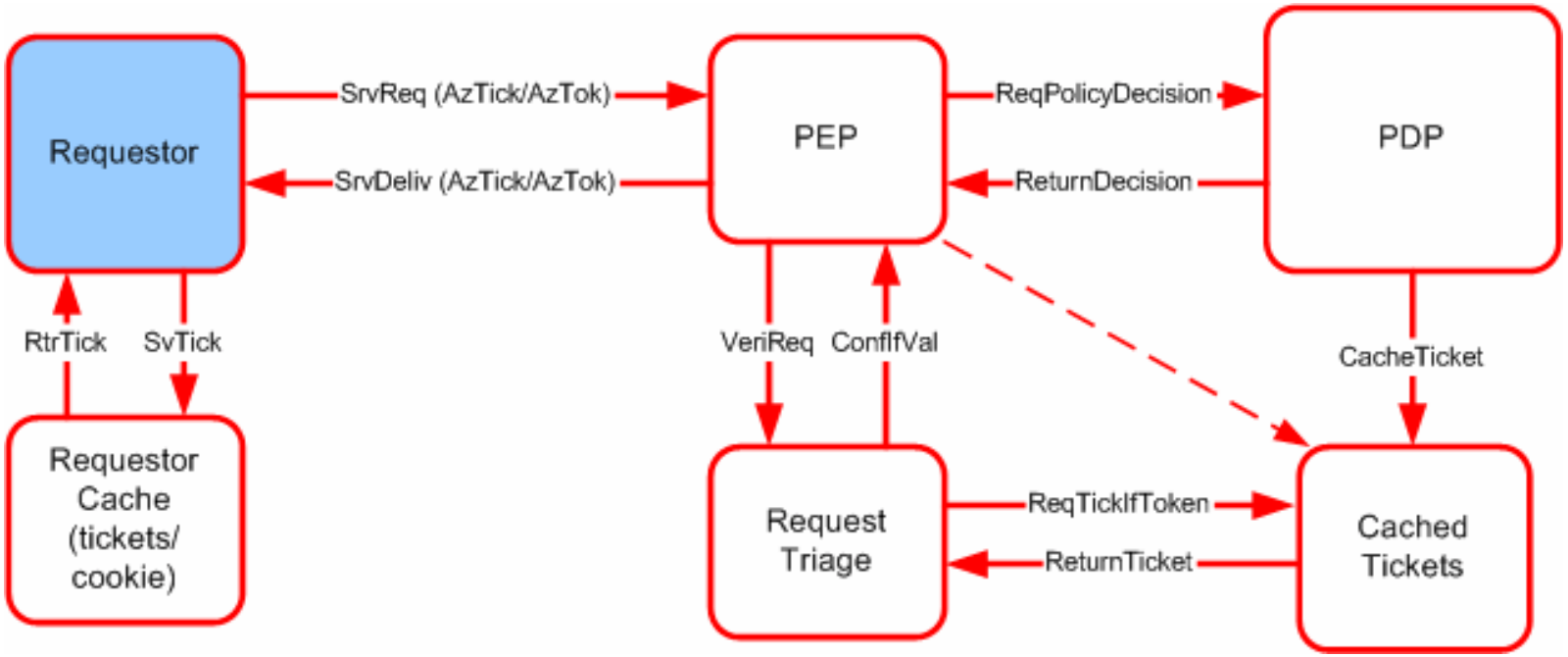
PDP Configuration

- Standard XACML PDP configuration
- *In development:* Master PDP configuration with components and Request/policy evaluation (micro)flow

AuthZ Session management in GAAA-RBAC

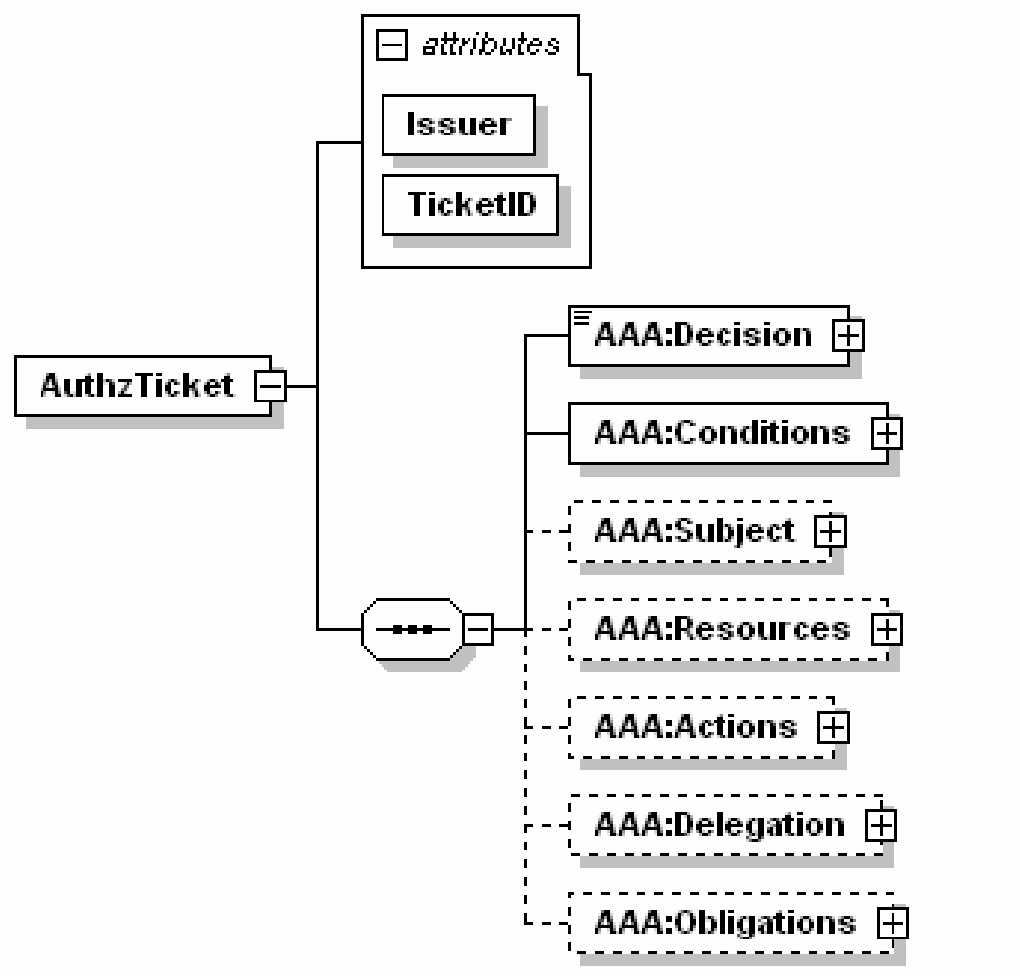
- Maintaining session is a part of generic RBAC functionality
- Session can be started only by authorised Subject/Role
  - Session can be joined by other less privileged users
  - Session related permissions can be delegated according to the Delegation policy
- SessionID is included into AuthzTicket together with other decision attributes
  - Signed AuthzTicket is cached by PEP or PDP
- If session is terminated, cached AuthzTicket is deleted
  - Note: AuthzTicket revocation should be done globally for the AuthZ trust domain

Tickets/Tokens handling in AuthZ system



- AuthzTicket is issued by PDP and may be issued by PEP
- AuthzTicket must be signed
- AuthzTicket contains all necessary information to make local PEP-Triage Request verification
- When using AuthzTokens, AuthzTickets must be cached; Resolution mechanism from token to ticket must be provided

AuthZ ticket for extended security context management – Data model (1) - Top elements



AuthZ ticket main elements

<Decision> element - holds the PDP AuthZ decision bound to the requested resource or service expressed as the ResourceID attribute.

<Conditions> element - 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> element - holds obligations that PEP/Resource should perform in conjunction with the current PDP decision.

AuthZ ticket format (proprietary) for extended security context management

```
<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

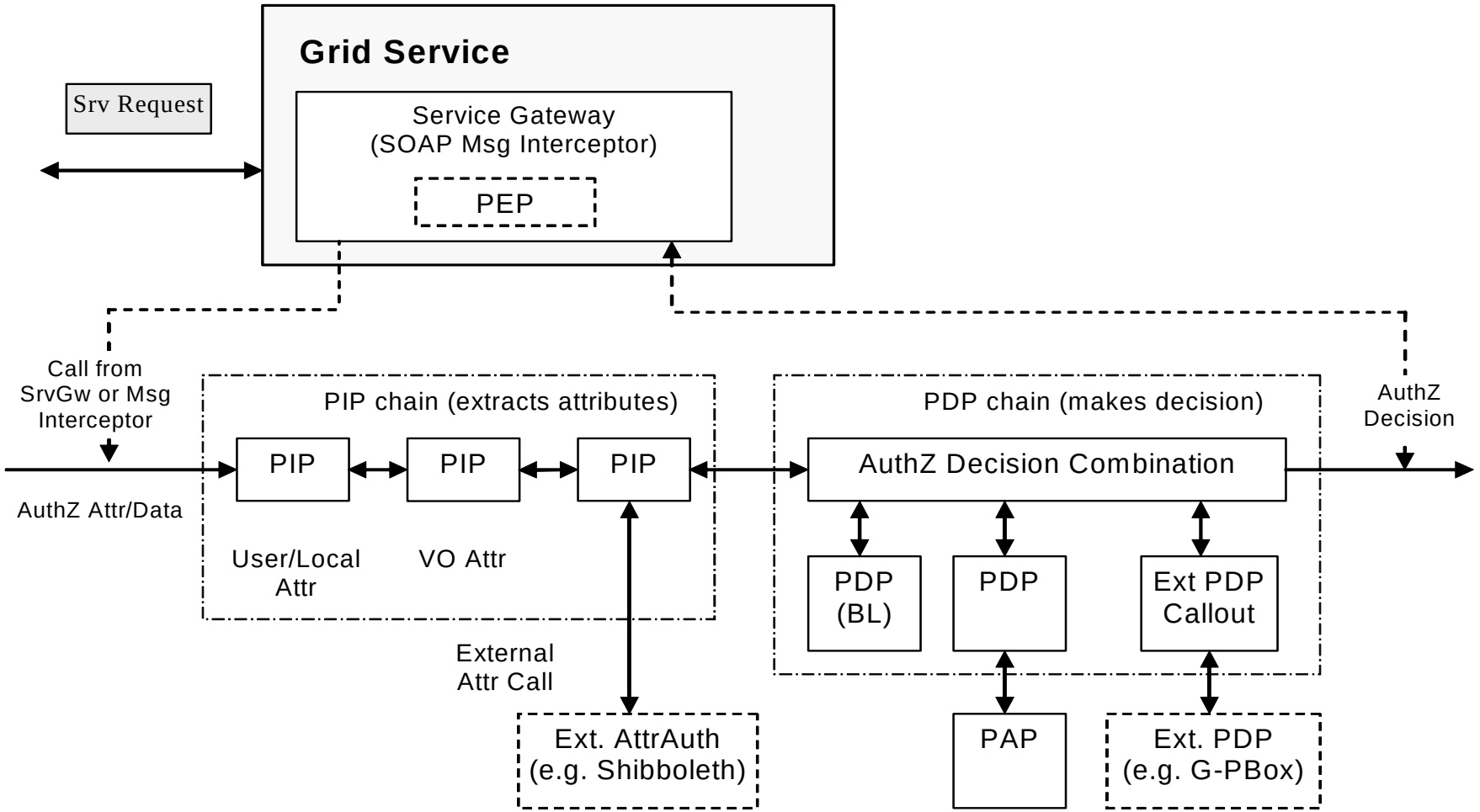
Future developments

- General – integration with BPEL-based WFMS
  - To provide extended configuration/context management functionality to interact with the WFMS
- Extending GAAAPI/GAAA_tk
  - to support different credentials format and callouts by using GT4-AuthZ and gJAF libraries
  - Adding external callouts to Attribute services and Credential Validation Service (CVS)
- Integration with existing access control tools GT4-AuthZ, gJAF, Acegi
- AuthZ session management with the extended AuthZ ticket functionality
  - including delegation and complex and obligated policy decisions

Additional information

- gJAF components and interaction with the Grid service/application
- XACML policy examples
- VO and dynamic security associations

gJAF components and connection to the Grid Service

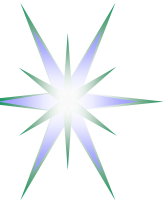


RBAC models - Reference

Source Sandhu et al.: Role-Based Access Control Models

http://www.list.gmu.edu/journal_papers1.htm

- RBAC0 – flat role-permissions model
  - One user per session (single or multiple roles)
  - One user can have multiple sessions
- RBAC1 – roles hierarchy and capabilities inheritance
  - One user per session (dominant roles can be added)
- RBAC2 = RBAC0 + constraints
  - Enforces high-level (local) policies
  - Decentralised security model and context -dependent
- RBAC3 = RBAC1 + constraints



XACML Special profiles for RBAC and complex Resources

XACML RBAC profile

- defines policies that require multiple Subjects and roles combination to access a resource and perform an action
- implements hierarchical RBAC model when some actions require superior subject/role approval to perform a specific action
- can significantly simplify rights delegation inside the group of collaborating entities/subjects

XACML Hierarchical Resource profile

- defines policy format for hierarchically organised resources, e.g. file system or XML-based repositories

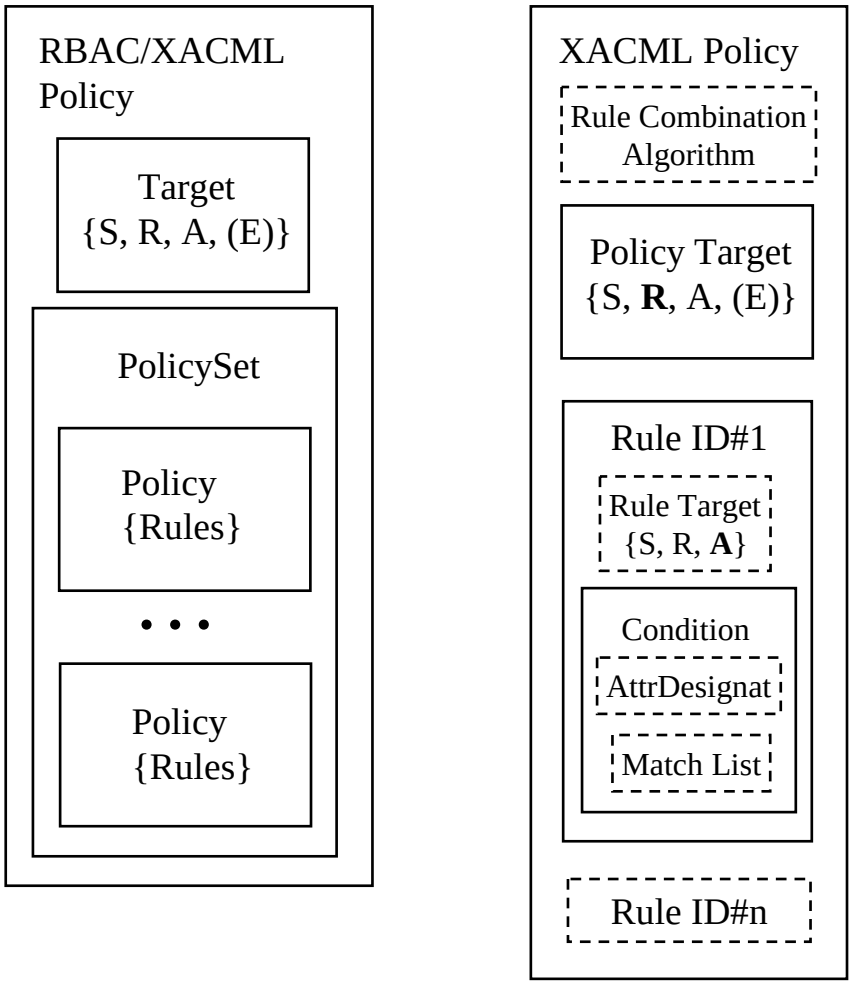
XACML complex Resource profile

- allows for complex request to multiple resources having the same request context, however decision is provided per resource

XACML3 Delegation profile

XACML Policy structure

XACML Policy format



CNL AuthZ policy: XACML Policy generation conventions

- Policy Target is defined for the Resource
- Policy combination algorithm is “ordered-deny-override” or “deny-override”
- Rule Target is defined for the Action and may include Environment checking
  - Rule’s Condition provides matching of roles which are allowed to perform the Action
- Access rules evaluation
  - Rules are expressed as permissions to perform an action against Subject role
  - Rule combination algorithm “permit-override”
  - Rules effect is “Permit”
- Subject and Credentials validation – is not supported by current XACML functionality
  - Credential Validation Service (CVS) – proposed GGF-AuthZ WG development

RBAC AuthZ policy: Resource, Actions, Subject, Roles

Actions (8)

- StartSession
- StopSession
- JoinSession
- ControlExperiment
- ControlInstrument
- ViewExperiment
- ViewArchive
- AdminTask

Roles (4)

- Analyst
- Customer
- Guest
- Administrator
- (CertifiedAnalyst)

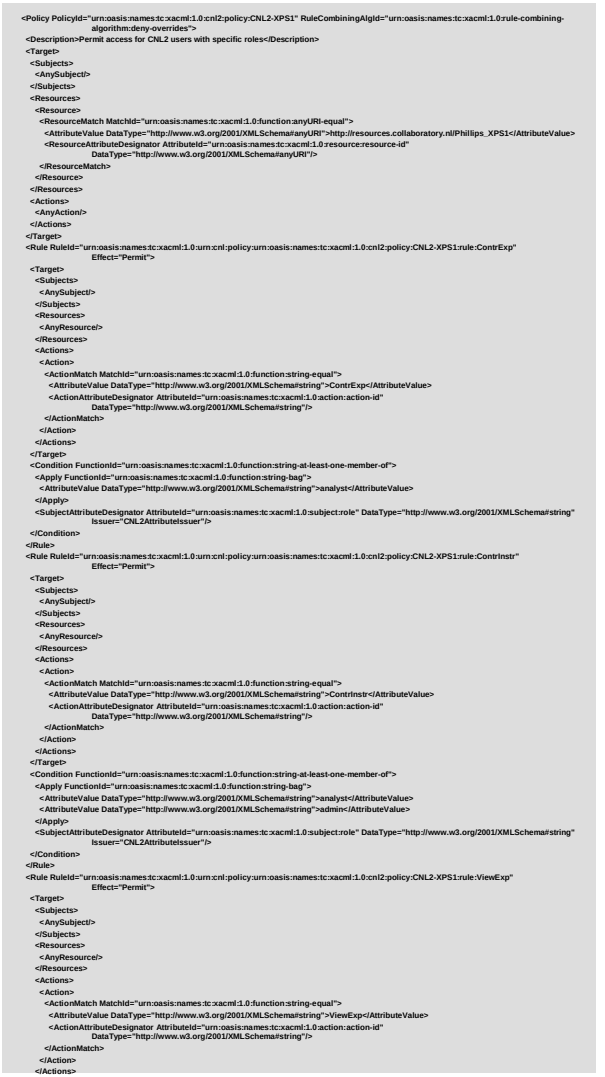
Naming convention

- Resource - “http://resources.collaboratory.nl/Phillips_XPS1”
- Subject – “WHO740@users.collaboratory.nl”
- Roles - “role“ or “role@ExperimentID”

Simple Access Control table

Roles	Anlyst	Custm	Guest	Admin
ContrExp	1	0	0	0
ContrInstr	1	0	0	1
ViewExp	1	1	1	0
ViewArch	1	1	0	1
AdminTsk	0	0	0	1
StartSession	1	0	0	0
StopSession	1	0	0	1
JoinSession	1	1	1	0

See XACML policy example =>

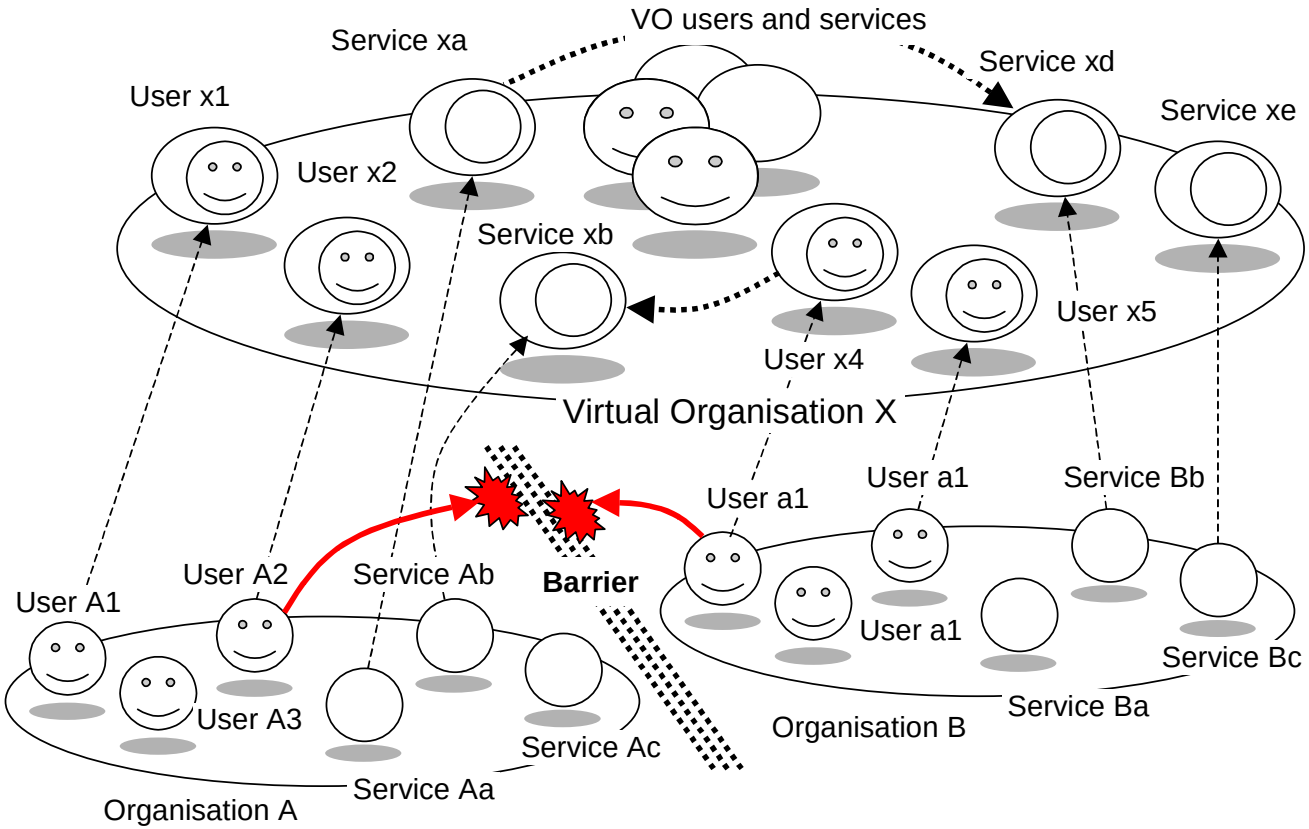


```
<Policy PolicyId="urn:oasis:names:tc:xacml:1.0:cnl2:policy:CNL2-XPS1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
                algorithm:deny-overrides">
 <Description>Permit access for CNL2 users with specific roles</Description>
 <Target>
  <Subjects>
   <AnySubject/>
  </Subjects>
  <Resources>
   <Resource>
    <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://resources.collaboratory.nl/Phillips_XPS1</AttributeValue>
     <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    </ResourceMatch>
   </Resource>
  </Resources>
  <Actions>
   <AnyAction/>
  </Actions>
 </Target>
 <Rule RuleId="urn:oasis:names:tc:xacml:1.0:urn:cnl:policy:urn:oasis:names:tc:xacml:1.0:cnl2:policy:CNL2-XPS1:rule:ContrExp"
                Effect="Permit">
  <Target>
   <Subjects>
    <AnySubject/>
   </Subjects>
   <Resources>
    <AnyResource/>
   </Resources>
   <Actions>
    <Action>
     <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ContrExp</AttributeValue>
      <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
     </ActionMatch>
    </Action>
   </Actions>
  </Target>
  <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">analyst</AttributeValue>
   </Apply>
   <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role" DataType="http://www.w3.org/2001/XMLSchema#string"
                Issuer="CNL2AttributeIssuer"/>
  </Condition>
 </Rule>
 <Rule RuleId="urn:oasis:names:tc:xacml:1.0:urn:cnl:policy:urn:oasis:names:tc:xacml:1.0:cnl2:policy:CNL2-XPS1:rule:ContrInstr"
                Effect="Permit">
  <Target>
   <Subjects>
    <AnySubject/>
   </Subjects>
   <Resources>
    <AnyResource/>
   </Resources>
   <Actions>
    <Action>
     <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ContrInstr</AttributeValue>
      <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
     </ActionMatch>
    </Action>
   </Actions>
  </Target>
  <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">analyst</AttributeValue>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">admin</AttributeValue>
   </Apply>
   <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role" DataType="http://www.w3.org/2001/XMLSchema#string"
                Issuer="CNL2AttributeIssuer"/>
  </Condition>
 </Rule>
 <Rule RuleId="urn:oasis:names:tc:xacml:1.0:urn:cnl:policy:urn:oasis:names:tc:xacml:1.0:cnl2:policy:CNL2-XPS1:rule:ViewExp"
                Effect="Permit">
  <Target>
   <Subjects>
    <AnySubject/>
   </Subjects>
   <Resources>
    <AnyResource/>
   </Resources>
   <Actions>
    <Action>
     <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ViewExp</AttributeValue>
      <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
     </ActionMatch>
    </Action>
   </Actions>
  </Target>
  <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">analyst</AttributeValue>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">customer</AttributeValue>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">guest</AttributeValue>
```

VO in Collaborative applications and Complex resource provisioning

- VO based functionality (and requirements) to support dynamic security associations
  - Dynamic Trust management
    - Establishing dynamic trust management relations between VO members
  - Attribute and metadata resolution and mapping
    - VO-based access control service requires common VO-wide attributes that however can be mapped to the original ones
  - Policy combination and aggregation
    - To allow conflict resolution and policy harmonisation between VO members
  - Flexible/distributed VO management infrastructure

VO bridging inter-organisational barriers



VO allows bridging inter-organisational barriers without changing local policies

- Requires VO Agreement and VO Security policy
- VO dynamics depends on implementation but all current implementations are rather static

Dynamic Security Associations

- **Session** – establishes security context in the form of session key that can be a security token or simple UID bound to secure credential/context
  - Session may associate/federate users, resources and actions/processes
- **Job/workflow** – more long-lived association and may include few sessions
  - May need to associate more distributed collection of users and resources for longer time required to deliver a final product or service
  - Job and workflow may contain decision points that switch alternative flows/processes
  - Security context may change during workflow execution or Job lifetime
  - Job description may contain both user and resource lists and also provide security policy and trust anchor(s) (TA)
- **Project or mission oriented cooperation** – established for longer time cooperation (involving people and resources) to conduct some activity
  - This is actually the area of currently existing VO associations
- **Inter-organisational association or federation** – established for long-term cooperation, may have a wide scope of cooperative areas
  - This is the area of inter-university associations
    - Shibboleth Attribute Authority Services (SAAS) is designed for this kind of federations