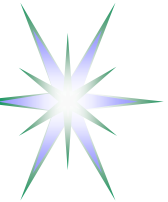
Policy Based Access Control in Dynamic Grid-based Collaborative Environment

COLSEC'06 Workshop, CTS2006 Conference
14-17 May 2006, Las Vegas

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



Outline

- Background – Origin of this work and contributing projects
- Collaboratory.nl project overview and status
- Workflow and Security context management in Experiment-centric collaborative environment
- GAAA-RBAC profile – design and implementation suggestions
- Using XACML for policy expression in GCE applications
- Future developments
- Additional materials (technical)

Background – Origin of this work

- This work is a result of ongoing development of the Generic Authentication, Authorisation, Accounting (GAAA) Authorisation Framework (GAAA-AuthZ) for Grid-based Collaborative Environment (GCE)
- Typical Grid-based collaborative environment
  - Dynamic - since the environment can potentially change from one experiment to another
  - Multidomain - may span multiple administrative and trust domains
    - must handle different user identities and attributes/privileges that must comply with different policies (both experiment and task specific, and site-local)
  - Customer-driven
  - Human controlled and interactive

Background – Contributing projects

- EU project EGEE (Enabling Grid for E-sciencE)
  - Knowledge and experience of up-to-date Grid technologies
  - GT4-AuthZ based gLite Authorisation Framework
  - Operational security and Grid Vulnerability analysis
- National projects VL-e (Virtual Laboratory for e-Science) and Gigaport-NG (New Generation)
  - Architecture and implementation for distributed Access Control infrastructure
- Industry funded project Collaboratory.nl (CNL)
  - Central Authorisation service – architecture and implementation

Collaboratory.nl project Overview - Used technologies and development platform

Collaboratory.nl project at its stage CNL3 – industry prototype

- Industry level software and new challenges for research

Development platforms

- GridSphere – extensible portlet based portal framework
  - Create virtual working environment
  - Manage Instrument
- Eclipse Rich Client Platform (RCP)
  - Extensive range of plugins and libraries for collaborative applications
    - chat, whiteboard, videostreaming, etc.
  - Rapidly developing platform
- Acegi security for Spring
  - Interceptor service plugins/callouts (aspect-oriented programming)
    - Internal ACL and callouts to external AuthZ modules, e.g. GAAA-AuthZ

CNL3 domain model – Resource hierarchy and services context

Facility > Virtual Lab > Experiment > Experiment/Collaborative Session

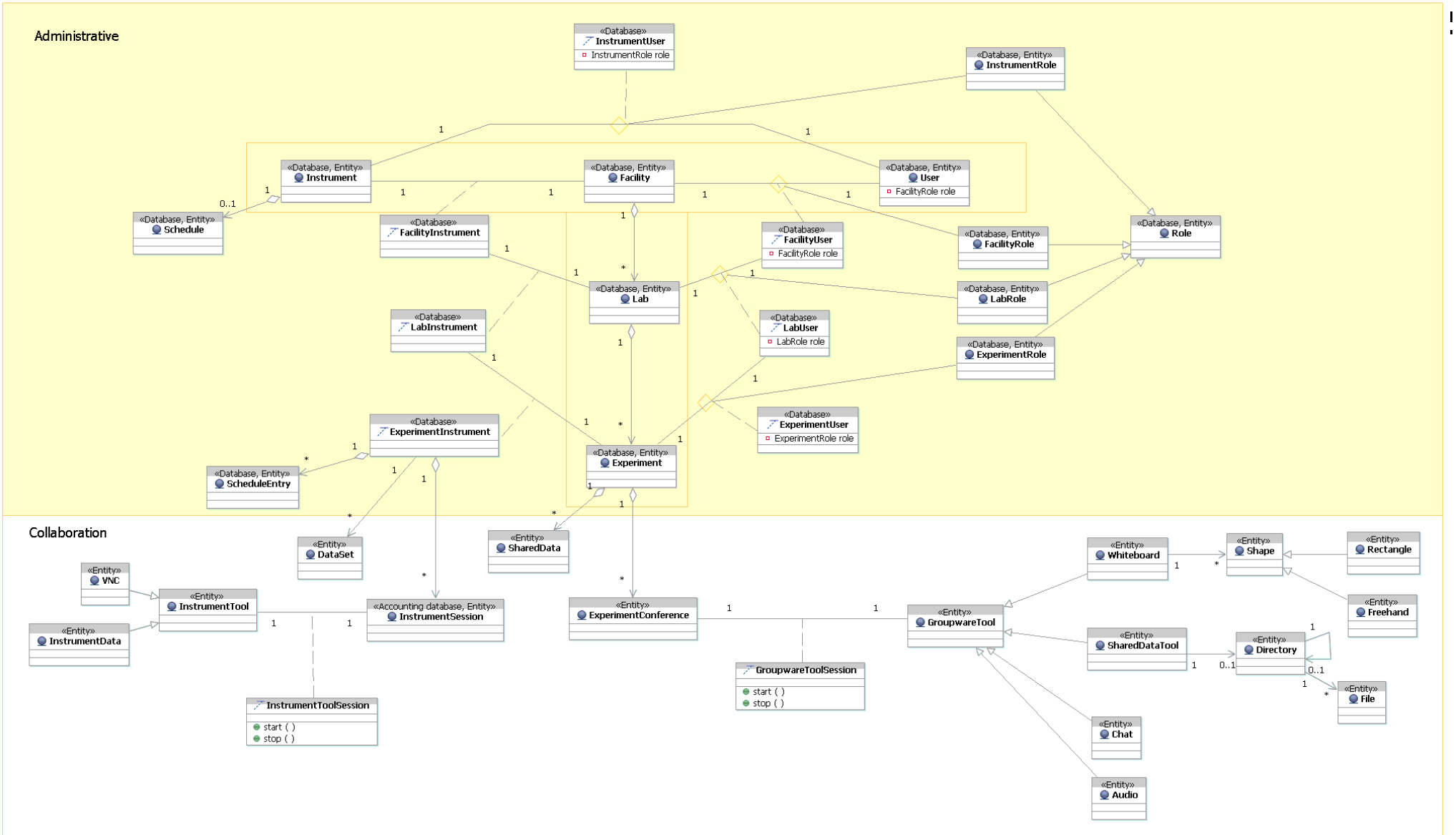
- Provides context for
  - Instrument as the access object Resource
  - User roles/attributes
- Users as registered users at hosted Facility or member Facility
- Access control policy/rules depend on the domain context and experiment stage and/or collaborative session

Two solutions/mechanisms to flexibly manage security context

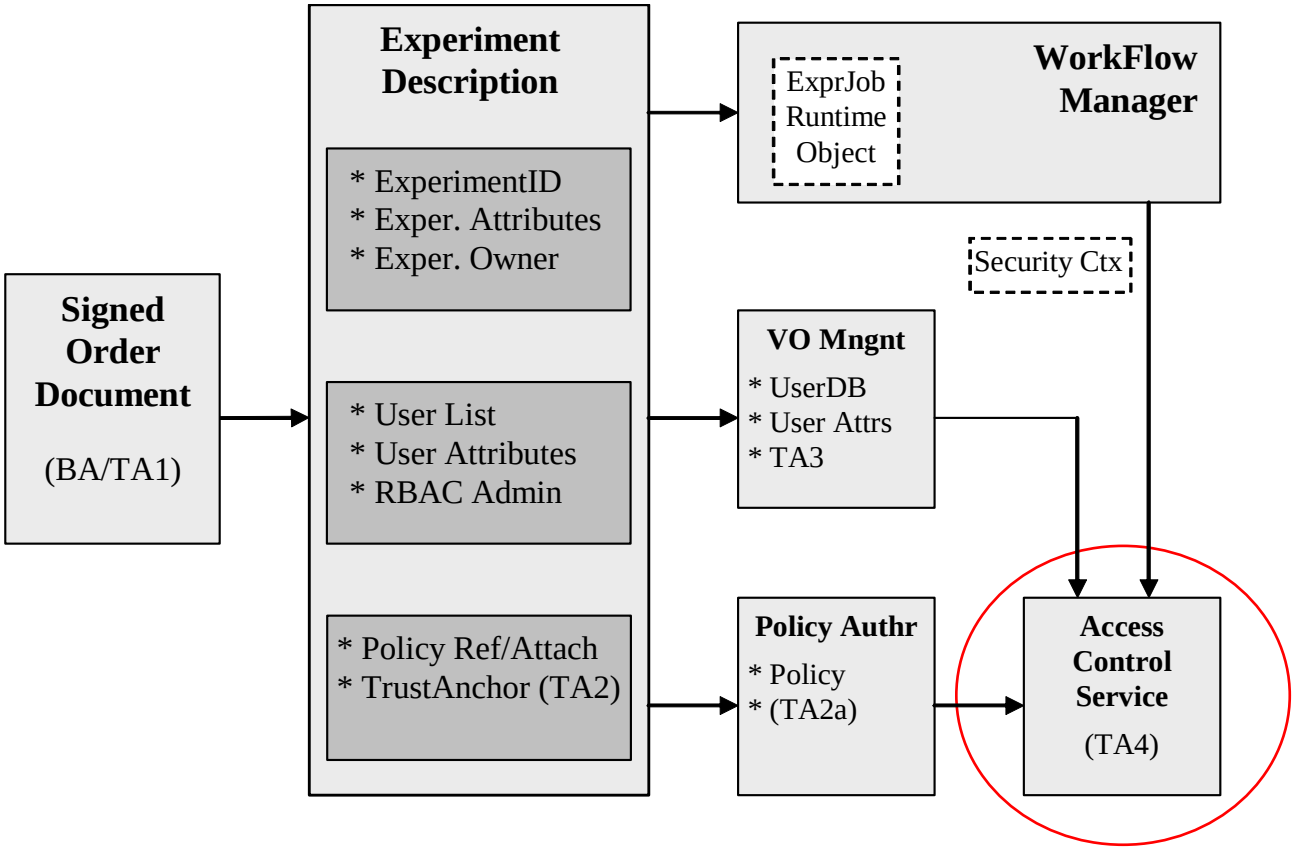
- Experiment workflow
- Context aware Access control infrastructure

CNL3 Domain model

CNL3 Domain Model



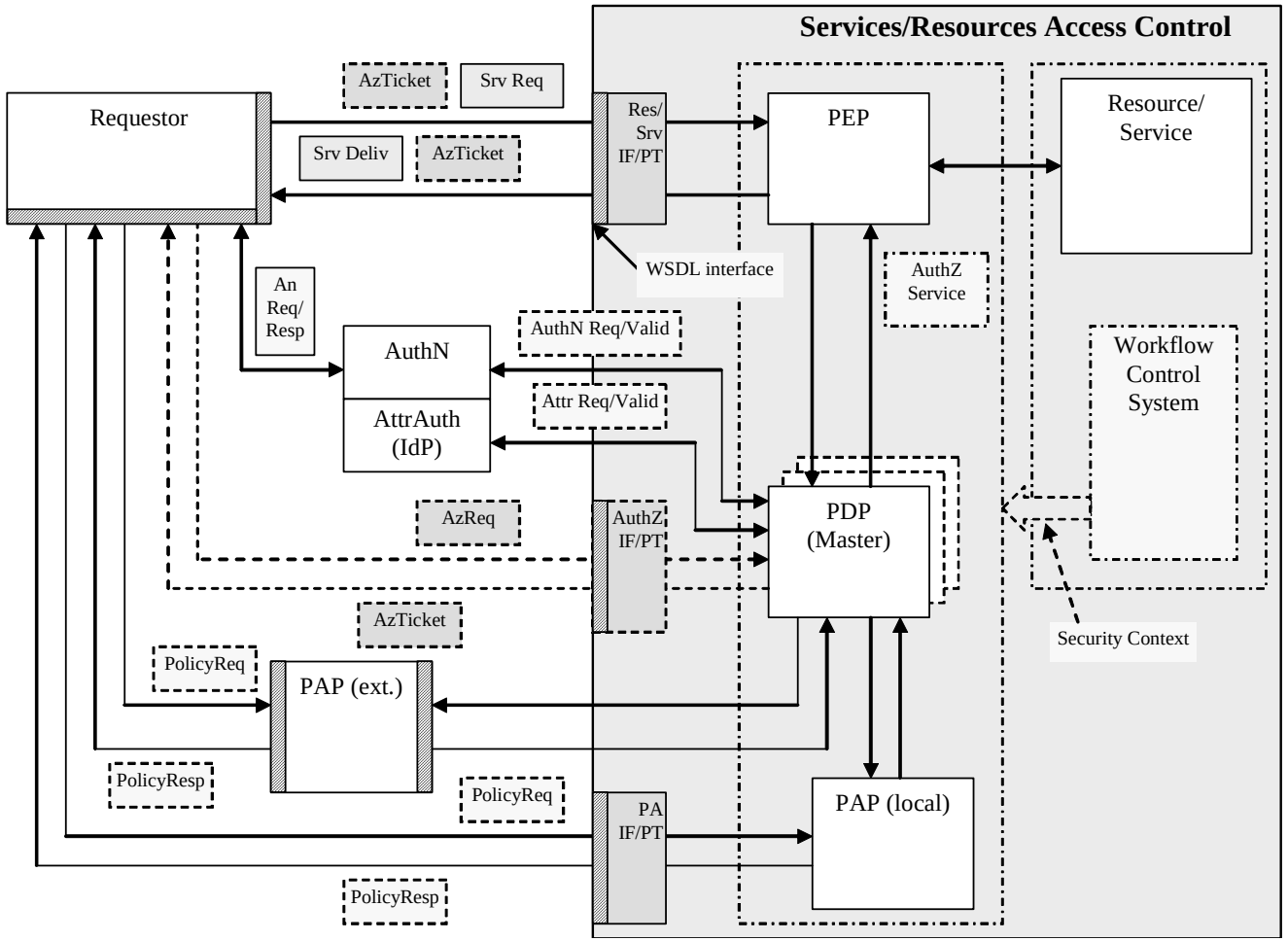
CNL3 Experiment-centric security model and using workflow for security context management



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)

Moving to Grid/Web Service platform



- 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 can fetch policy document and apply restrictions/rules to elements, which declared policy compliance requirements

Security context management: Changing information and suggested mechanisms

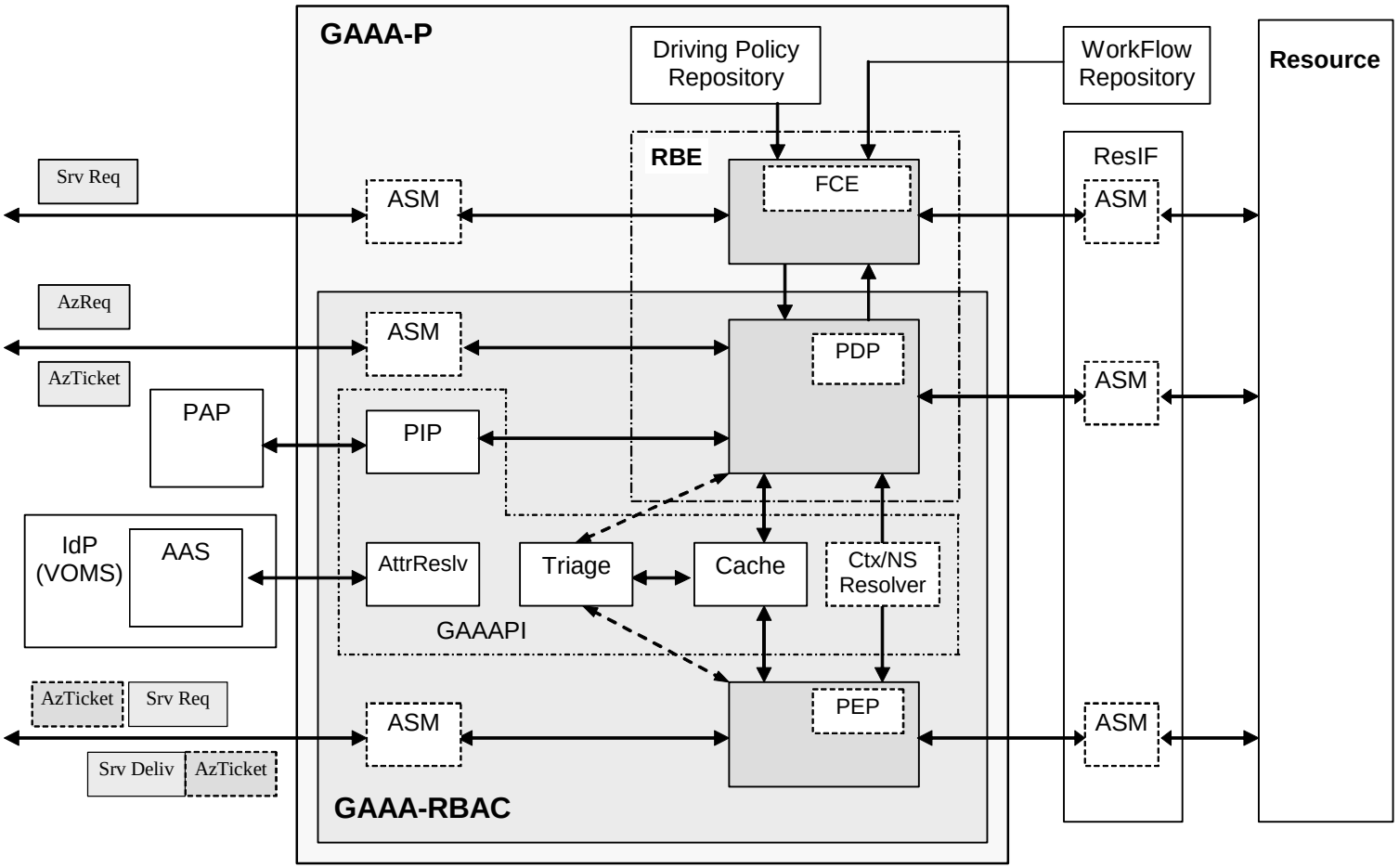
Context dependent information/attributes:

- Service/Resource environment/domain
- Policy
- Trust domains and authorities
- Attribute namespace
- Credential format

Mechanisms to communicate/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/booked 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**

GAAA-RBAC profile components

- GAAA-RBAC profile consists of two generic modules: Policy Decision Point (PDP) for individual policies evaluation and Policy Enforcement Point (PEP) for policy decision enforcement
- GAAAPI provides all necessary functionality for communication between PEP and PDP and providing security context for service request evaluation
  - Namespace resolver to define/resolve what policy and what attributes should be used for the request evaluation
  - Triage (together with Cache) used for AuthZ tickets/tokens handling and AuthZ session management
    - provides local to PEP service request evaluation
  - Attribute resolver and Policy Information Point (PIP) provide resolution and call-outs to related authoritative Policy Authority Points (PAP) and Attribute Authority Service (AAS)
    - May call external Credential Validation Service (CVS)

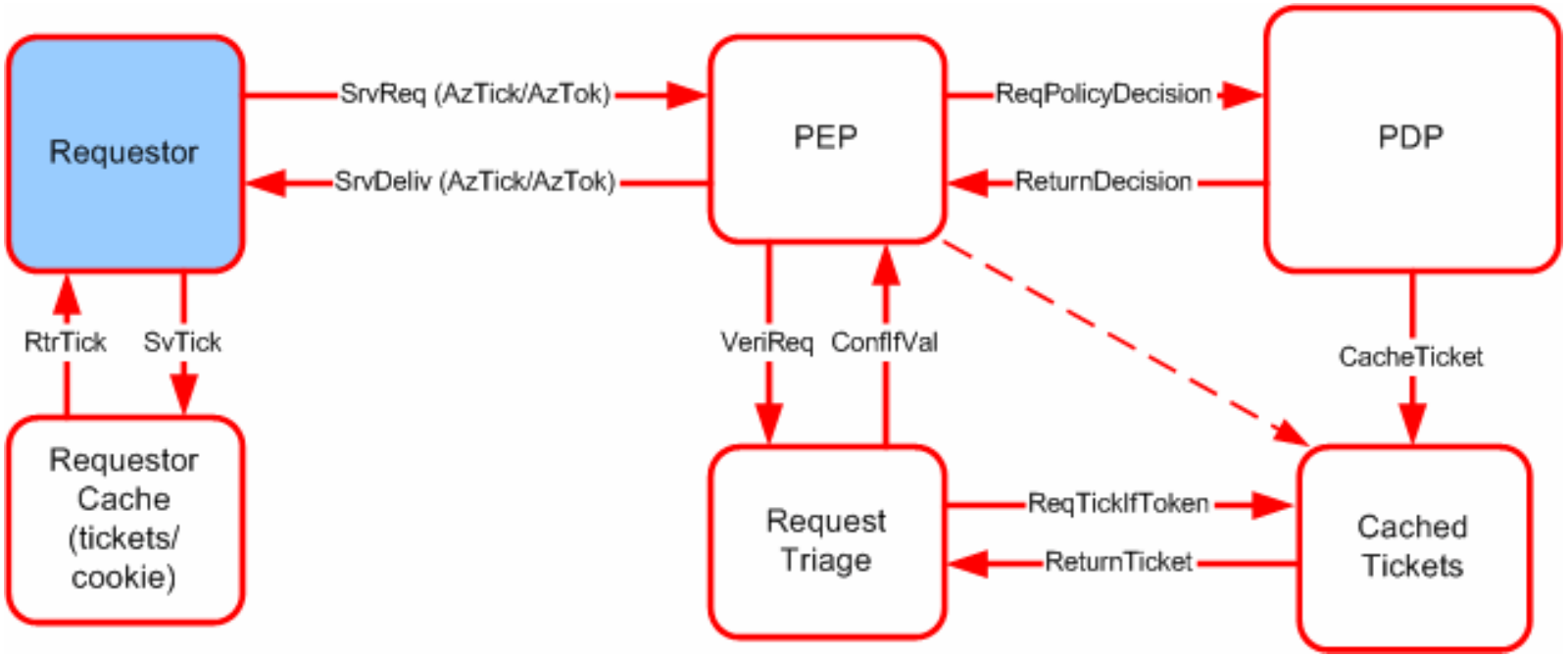
GAAA-RBAC for CNL3 and Grid-based Collaborative Environment

- Experiment-centric domain security model for virtualised GCE
  - CNL3 domain based security context
  - Experiment workflow for dynamic security context management
- Extended RBAC functionality based on GAAA Authorisation framework
  - XACML Request/Response messaging
    - External callouts using SAML protocol
  - XACML policy and XACML PDP
- Authorisation service performance optimisation using tickets/tokens
  - Proprietary and SAML based AuthzTicket format
  - AuthZ Session management
  - Delegation and Session credentials renewal
- Trust domains and credential authorities configuration
  - AuthN service, Attribute Authorities, AuthZ tickets authority, PEP/PDP keys

Session management in GAAA-RBAC

- Maintaining AuthZ session is a part of the generic RBAC functionality
- Session can be started only by authorised Subject/Role
  - Session can be joined by other less privileged users
- SessionID is included into AuthzTicket together with other decision attributes
  - Signed AuthzTicket is cached by issuing 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



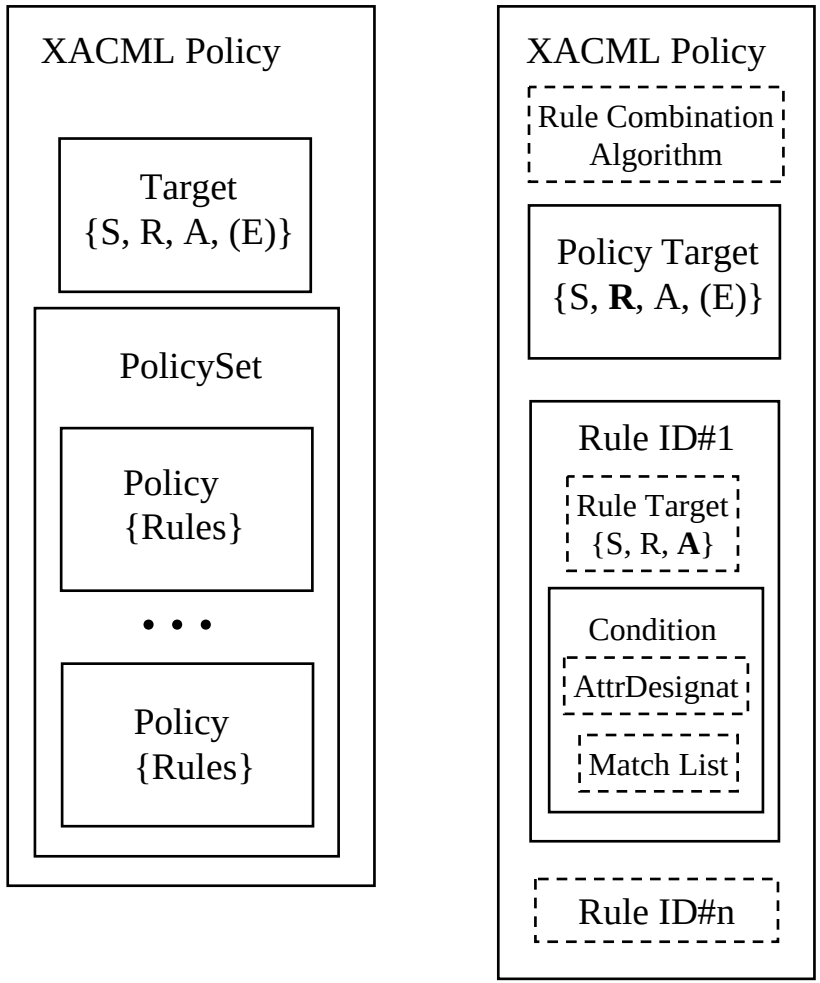
- AuthzTicket is issued by PDP and may be issued by PEP
- AuthzTicket must be signed
- AuthzTicket contains all necessary information to make local PEP-Triage Request verification
- When using AuthzTokens, AuthzTickets must be cached; Resolution mechanism from token to ticket must be provided

GAAA AuthzTicket format

```
<cnl:CNLAuthzTicket xmlns:AAA="" xmlns:cnl="http://www.aaauthreach.org/ns/#CNL"
   Issuer="urn:cnl:trust:tickauth:pep" PolicyURIs="CNL3policy01-test"
   SessionIndex="sessionID-2006-03-23-test" TicketID="e916c88a86462d0e26cd4faae1de88ae">

   <cnl:Decision
   ResourceID="http://resources.collaboratory.nl/Phillips_XPS1">Permit</cnl:Decision>

   <cnl:Validity NotBefore="*" NotOnOrAfter="**" renewal="yes/no"/>
   <cnl:Delegation> <cnl:Community/> <cnl:Subjects/> </cnl:Delegation>

   <cnl:Subject Id="subject">
        <cnl:SubjectID>WHO740@users.collaboratory.nl</cnl:SubjectID>
        <cnl:SubjectConfirmationData>IGhA11vwa8...W4U=</cnl:SubjectConfirmationData>
        <cnl:Role>analyst</cnl:Role>
        <cnl:SubjectContext>ExperimentID::CNL2-XPS1-2006-02-02</cnl:SubjectContext>
   </cnl:Subject>

   <cnl:Resource>http://resources.collaboratory.nl/Phillips_XPS1</cnl:Resource>

   <cnl:Actions> <cnl:Action>ControlInstrument</cnl:Action> </cnl:Actions>

   <ds:Signature> <ds:SignedInfo>     <ds:SignatureValue> </ds:Signature>
</cnl:CNLAuthzTicket>
```

XACML Policy format

- Policy target is defined for the triad Subject-Resource-Action and may include Environment
- Policy may contain Obligation element that defines actions to be taken by PEP on Policy decision by PDP



CNL3 AuthZ policy: XACML Policy generation conventions

- Policy Target is defined for the Instrument (containing also CNL domain information)
- 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

Example CNL2 AuthZ policy: Resource, Actions, Subject, Roles

Actions (8)

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

Roles (4)

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

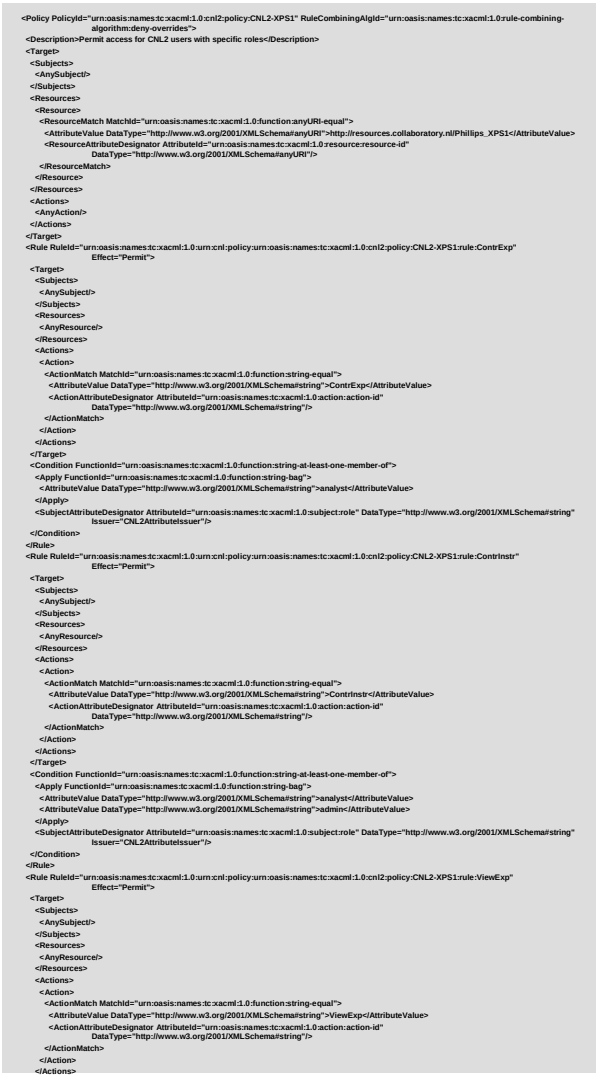
Naming convention

- Resource - “http://resources.collaboratory.nl/**<CNLdomain>**/Phillips_XPS1”
- Subject – “WHO740@**<CNLdomain>.**users.collaboratory.nl”
- Roles - “role“ or “role@**<CNLdomain>**.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>
```

Considering XACML special profiles for flexible policy expression

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

XACML3 Delegation profile

Will depend on available XACML/PDP implementation

Future developments

- Integration with existing access control tools
  - GT4 Authorization Framework
  - Acegi (in context of CNL3+)
- Extending GAAA_tk to support different credentials format and callouts
  - Adding external callouts to Attribute services and Credential Validation Service (CVS)
  - Adding support for VOMS credentials – to allow VO-based user and resource attributes management
- Dynamic Security Context management
  - Extend RBAC/XACML model and redesign GAAA_tk components
  - Adding Security features to popular workflow management tools, e.g. BPEL

GAAA_tk: Integration with GT4 AuthZ framework

GT4 Authorisation Frameworks (GT4-AuthZ) provides access control for Grid services

- Can be applied at the level of container, service, or resource/application
- Implemented access control PDP's
  - Access Control Lists (ACL), gridmap file, identity or host based, simple XACML based PDP
- external policy evaluation callouts using OGSA Authorisation PortType
- Support for different types of secure credentials
  - X.509 Proxy and Attribute Certificates, VOMS credentials
- Support for WS-Trust based secure communication

Suggested GAAA_tk contribution

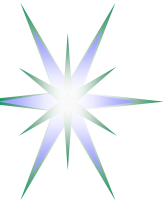
- Complex XACML policies evaluation
- Authorisation session support using AuthZ tickets and tokens handling
- Flexible request semantics and trust domains configurations and management

Integration can be done in three ways

(1) using GT4 WS/messaging middleware to provide WS-based access to GAAA_tk authorisation service to allow easy GAAA_tk integration into different applications

(2) adding GAAA AuthZ callouts to GT4 AuthZ framework

(3) integrating GAAA AuthZ PDP/GAAAPI into GT4-AuthZ as one of internal PDP's



Acknowledgements

This work results from the Collaboratory.nl project, a research initiative that explores the possibilities of remote control and use of advanced lab facilities in a distributed and collaborative industrial research setting. The Collaboratory.nl consortium consists of DSM, Philips, Corus, FEI, IBM, Telematica Instituut and the University of Amsterdam.

This work is a part of ongoing research and development of the Generic AAA Authorisation framework by the System and Network Engineering Group at the University of Amsterdam.

Additional information

- RBAC models and XACML implementation
- Interacting components and entities in the Experiment-centric security model
- Detailed AuthZ and AuthN ticket and token examples

CNL3: Building integrated manageable Access Control Infrastructure

- Needs for central/integration point
  - Business Agreement, or
  - Experiment, or
  - Job
- To allow integration of all security entities and components during the whole experiment lifetime
  - Users (and resources)
  - Policy
  - Trust
  - Execution environment and security context

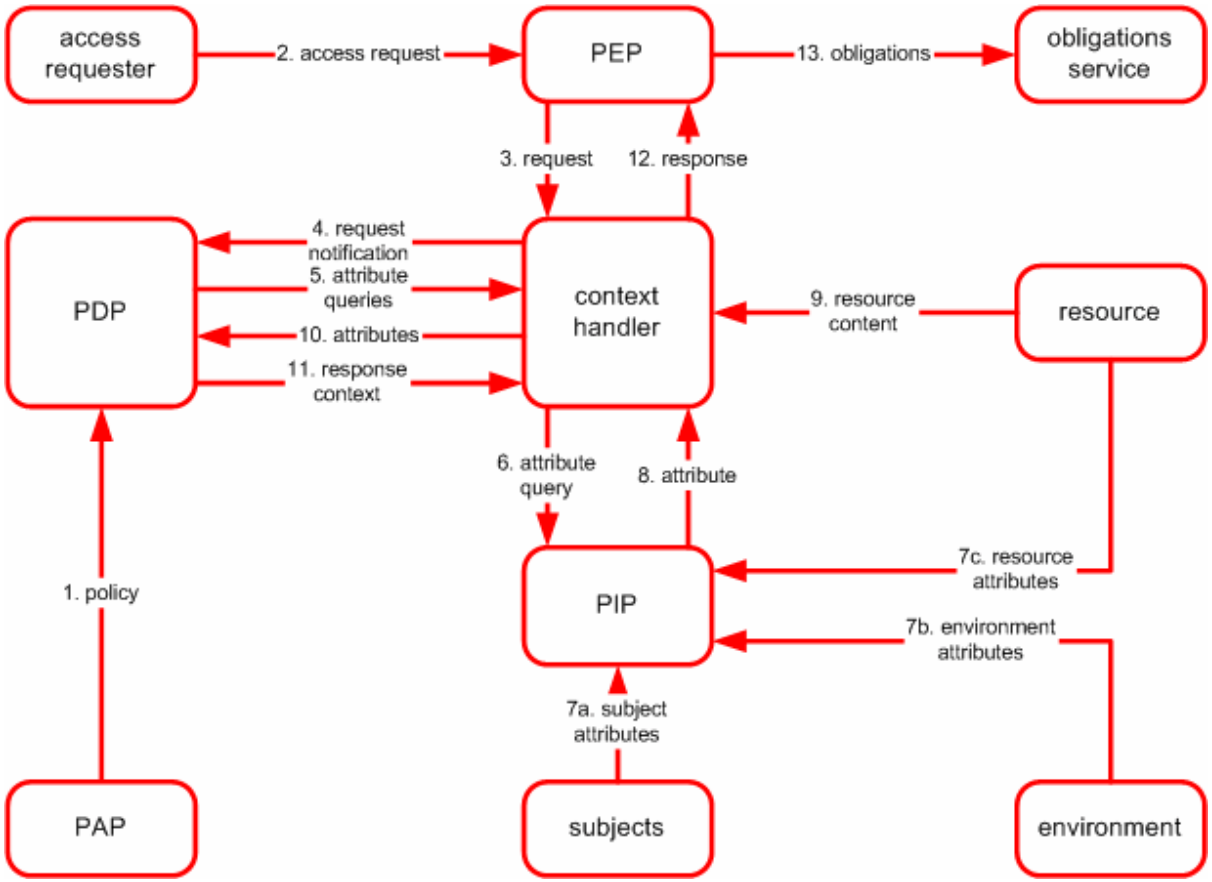
RBAC models - Reference

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 RBAC model: main components and dataflow



PEP/AEF - Policy Enforcement Point

PDP/ADF - Policy Decision Point

PIP - Policy Information Point

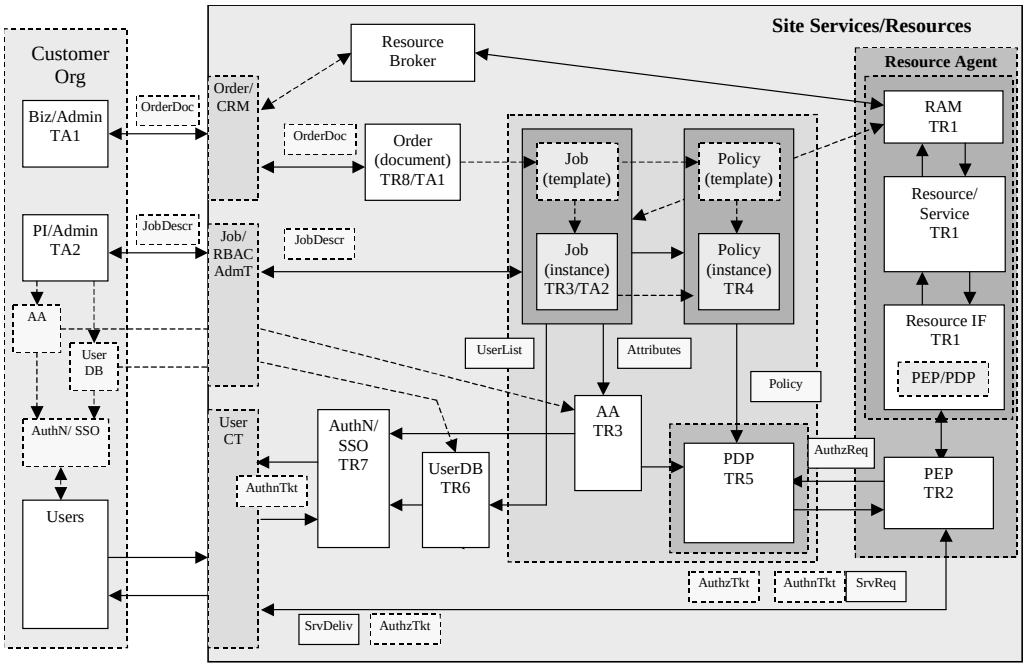
AA - Attribute Authority

PAP - Policy Authority Point

Internal model for Sun XACML reference library operations

- PDP, PolicyFinder
  - Combination Algorithms
- PIP/Context Handler
  - AttributeFinder, ResourceFinder, AttributeProxy

Trust relations in distributed access control infrastructure



Trust/credentials chain and delegation between major modules:

```
User =>
  => HomeOrg.staff(TA2)
    => Job.members
      => Member.roles
        => Role.permissions
```

Obtaining required permissions to perform requested action by the user:

```
User => AuthN(HomeOrg.staff(TA2), Job.members) =>
            => AuthZ(Member.roles, Policy.permissions) =>
                    => Resource.permissions
```

CNLAuthzTicket example – 1011 bytes

```
<cnl:CNLAuthzTicket xmlns:AAA="http://www.AAAarch.org/ns/AAA_BoD"
   xmlns:cnl="http://www.aaauthreach.org/ns/#CNL" Issuer="http://www.AAAarch.org/servers/AAA"
   PolicyURIs="CNLpolicy01" SessionIndex="JobXPS1-2005-001"
   TicketID="c24d2c7dba476041b7853e63689193ad">
   <!-- Mandatory elements -->
   <cnl:Decision
   ResourceID="http://resources.collaboratory.nl/Philips_XPS1">Permit</cnl:Decision>
   <cnl:Validity NotBefore="2005-02-13T01:26:42.699Z" NotOnOrAfter="2005-02-
   14T01:26:42.699Z"/>
   <!-- Additional elements -->
   <cnl:Subject Id="subject">
     <cnl:SubjectID>WHO740@users.collaboratory.nl</cnl:SubjectID>
     <cnl:SubjectConfirmationData>SeDFGVHYTY83ZXxEdsweOP8Iok</cnl:SubjectConfirmationData>
     <cnl:JobID>CNL2-XPS1-2005-02-02</cnl:JobID>
     <cnl:Role>analyst@JobID;expert@JobID</cnl:Role>
   </cnl:Subject>
   <cnl:Resource>http://resources.collaboratory.nl/Philips_XPS1</cnl:Resource>
   <cnl:Actions>
     <cnl:Action>cnl:actions:CtrlInstr</cnl:Action>
     <cnl:Action>cnl:actions:CtrlExper</cnl:Action>
   </cnl:Actions>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ... </ds:Signature>
</cnl:CNLAuthzTicket>
```

CNLAuthzTicket XML Signature element – 957 bytes (total signed ticket 1968 bytes)

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
     <ds:Reference URI="">
       <ds:Transforms>
         <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
         <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
  20010315#WithComments"/>
       </ds:Transforms>
       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
       <ds:DigestValue>nrNrZZDiw/2aDnKXFEHSeoixnsc=</ds:DigestValue>
     </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue>
0IZt9WsJT6an+tIxhhTPtiztDpZ+iynx7K7X2Cxd2iBwCUTQ0n61Szv81DKllWsq75IsHfusnm56
zT3fhKU1zEUsob7p6oMLM7hb42+vjfvNeJu2roknhIDzruMrr6hMDsIfaotURepu7QCT0sADm9If
X89Et55EkSE9oE9qBD8=
   </ds:SignatureValue>

   <ds:KeyInfo> << ... snip ... >> </ds:KeyInfo>

</ds:Signature>
```

RSA <ds:KeyInfo> element – 1010 bytes

(total signed ticket with KeyInfo - 3078 bytes)

```
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
     MIICADCCAWkCBEGX/FYwDQYJKoZIhvcNAQEEBQAwRzELMAkGA1UEBhMCTkwxGTAXBgNVBAoTEENv
     bGxhYm9yYXRvcnkubmwxHTAbBgNVBAMTFEFBQXV0aHJlYWNoIFNlY3VyaXR5MB4XDTA0MTExNTAw
     NDYxNFoXDTA1MDIxMzAwNDYxNFowRzELMAkGA1UEBhMCTkwxGTAXBgNVBAoTEENvbGxhYm9yYXRv
     cnkubmwxHTAbBgNVBAMTFEFBQXV0aHJlYWNoIFNlY3VyaXR5MIGfMA0GCSqGSIb3DQEBAQUAA4GN
     ADCBiQKBgQDdDrBhVmr1nD9eqi7U7m4yjIRxfvjAKv33EpuajvTKHpKUgLjbcBC3jNJ4F7a0GiXQ
     cVbuF/aDx/ydIUJXQktvFxK0Sm77WVeSel0cLc1hYfUSAg4mudtfsB7rAj+CzNnVdr6RLFpS9YFE
     lv5ptGaNGSbwHjU02HnArEGL2K+0AwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBADHKqkOW4mP9DvOi
     bMvf4oqXTth7yv8o3Zol7+nqlB9Tqf/bVNLMk8vNo5fWRHbpnHIFFgTk31nrJf8kEZEofvwAeW9s
     1gQtYfs1oxvsMPKHxFjJDiZlLkHRViJl/slz5a7pkLqIXLRsPFRziTksemRXB/fT8KDzM14pzQZg
     HicO
    </ds:X509Certificate>
  </ds:X509Data>
  <ds:KeyValue>
    <ds:RSAKeyValue>
      <ds:Modulus>
     3Q6wYVZq9Zw/Xqou1O5uMoyEcX74wCr99xKbmo70yh6SlIC423AQt4zSeBe2tBol0HFW7hf2g8f8
     nSFCV0JLbxcStEpu+1lXknpdHC3NYWH1EgIOJrnbX7Ae6wI/gszZ1Xa+kSxaUvWBRJb+abRmjRkm
     8B41NNh5wKxBi9ivtAM=
      </ds:Modulus>
      <ds:Exponent>AQAB</ds:Exponent>
    </ds:RSAKeyValue>
  </ds:KeyValue>
</ds:KeyInfo>
```

CNLAuthzToken example – 293 bytes

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

CNLAuthzToken is constructed of the CNLAuthzTicket TicketID and SignatureValue

CNLAuthzToken use requires caching CNLAuthzTicket's

CNLSAMLAuthzTicket example – 2254 bytes

```
<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
     xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" AssertionID="c236b047d62db5cecec6b240996bcb90" IssueInstant="2005-02-
     15T14:53:23.542Z" Issuer="cnl:subject:CNLAAAauthority" Version="1.1">
  <Conditions NotBefore="2005-02-16T14:32:12.506Z" NotOnOrAfter="2005-02-17T14:32:12.506Z">
     <Condition xsi:type="typens:cnl:session-id">JobXPS1-2005-001</Condition>
     <Condition xsi:type="typens:cnl:policy-uri">CNLpolicy01</Condition>
  </Conditions>
  <AuthorizationDecisionStatement Decision="Permit" Resource="http://resources.collaboratory.nl/Philips_XPS1">
    <Action Namespace="urn:oasis:names:tc:SAML:1.0:action:cnl:action">cnl:actions:CtrlInstr</Action>
    <Action Namespace="urn:oasis:names:tc:SAML:1.0:action:cnl:action">cnl:actions:CtrlExper</Action>
    <Evidence>
      <Assertion AssertionID="f3a7ea74e515ffe776b10a7eef0119d7" IssueInstant="2005-02-15T14:53:23.542Z"
     Issuer="cnl:subject:CNLAAAauthority" MajorVersion="1" MinorVersion="1">
        <Conditions NotBefore="2005-02-15T14:53:11.745Z" NotOnOrAfter="2005-02-16T14:53:11.745Z"/>
        <AttributeStatement>
          <Subject>
            <NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
     NameQualifier="cnl:subject">WHO740@users.collaboratory.nl</NameIdentifier>
            <SubjectConfirmation>
              <ConfirmationMethod>signed-subject-id</ConfirmationMethod>                    ===➔ moved to attr in SAML 2.0
              <ConfirmationData>
             PBLIR0aZRtdZmq979lj8eDpJ5VT6BxxWBtSApC5BPnIsfHRUcOOpWQowXBw2TmOZdJGNzFWhMinz
              XU3/wSdLjv+siO2JGfyZ7U9eqkM0GqY8VizMl5uRuUAsrr7AIHv9/DP1ksJMNDZ5DnGosMc+Zyqn
              KogfMqhK+DKqPwfHF6U=</ConfirmationData>
            </SubjectConfirmation>
          </Subject>
          <Attribute xmlns:typens="urn:cnl" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance" AttributeName="AttributeSubject" AttributeNamespace="urn:cnl">
            <AttributeValue xsi:type="typens:cnl:job-id">CNL2-XPS1-2005-02-02</AttributeValue>            ===➔ level 5 element
            <AttributeValue xsi:type="typens:cnl:role">analyst@JobID;expert@JobID</AttributeValue>
          </Attribute>
        </AttributeStatement>
      </Assertion>
    </Evidence>
  </AuthorizationDecisionStatement>
</Assertion>
```