Policy Based Access Control
in
CNL3 Authorisation Service

(Grid-based Collaborative Environment)

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

Outline

- CNL2 Security and AuthZ service – Overview
  - Security requirements and design approach
  - Role Based Access Control (RBAC) and XACML policy examples
- General concept and approach
  - Access Control model built around Job/Experiment description
- GAAA-RBAC profile – design and implementation suggestions
  - Configuration and trust domains management
  - AuthZ session management
  - Using AuthZ tickets and tokens for performance optimisation
- Summary – Future development
- Additional materials (technical)

GCE/OCE specific security requirements

- Open/Grid-based Collaborative Environment specific security requirements
  - Human controlled and interactive
  - Dynamic and multidomain
  - Customer driven
  - Data protection: personal, experimental, and metadata

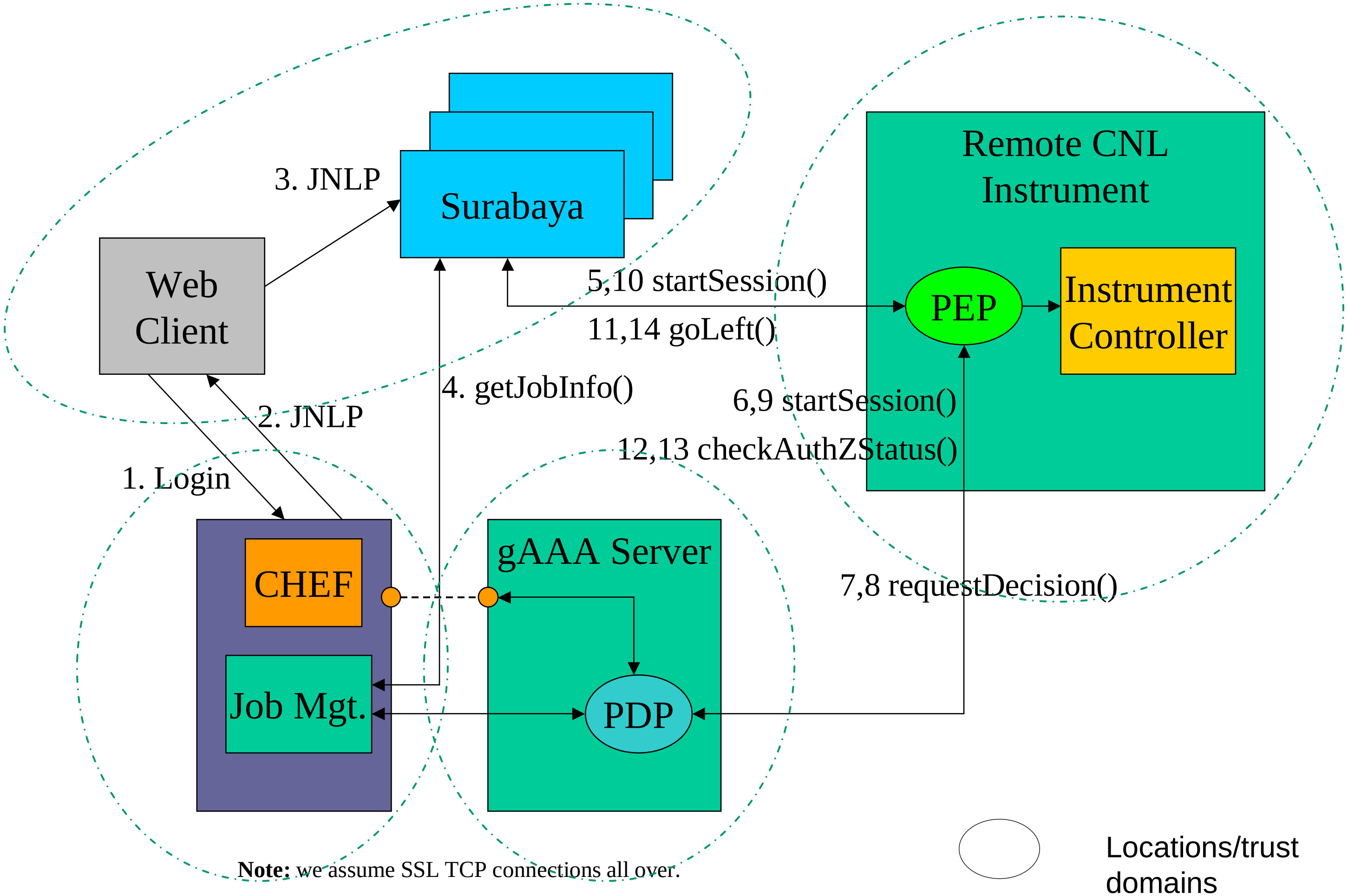
Design approach in CNL2 for AuthZ service

- Authorisation service design principles
  - Develop only new components not available in existing tools
  - Generic approach (using GAAA AuthZ framework)
  - Using standards and ensure compatibility with existing AuthZ/N tools and middleware platforms
- Compatibility and integration with existing access control tools
  - Policy formats mapping for flexible policy exchange and combination
  - GT4/gLite AuthZ Framework

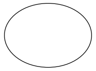
CNL2 Summary - Used technologies and new developments

- Job-centric security model that responds OCE dynamic distributed requirements
    - Job description format – intended to be compatible with WS-Agreement and JSDL (Job Submission Description Language)
- Extended RBAC functionality based on GAAA Authorisation framework
    - XACML Request/Response messaging
    - Migration from AAA policy expression format to XACML policy
- Authorisation service performance optimisation using tickets/tokens
    - Proprietary and SAML based AuthzTicket format
    - AuthZ Session management
- Trust model for distributed access control system and flexible key management
- XML Signature and XML Encryption for JobDescription and AuthzTicket security

Implementation: Authorisation Service operation in a CNL2 Demo system



Note: we assume SSL TCP connections all over.



JNLP – Java Network Launch Protocol

CHEF – Collaborative tool

Surabaya – Collaborative Workspace environment

Kizna SyncShare – realtime job management

Design conventions and agreements

- Key distribution and trust establishing
  - *Currently, in search of simple consistent model*
- Policy definition and format including subject, attributes/roles, actions semantics and namespaces
  - Compatibility with existing formats, e.g. SAML, XACML
  - Policy format defines/defined by the PDP implementation
- Secure credentials/ticket format
  - Standard vs proprietary
- Protocols and Messages format
  - SOAP + XACML Request/Response
  - SOAP + SAMLP + XACML

CNL2 AuthZ policy: Resource, Actions, Subject, Roles

Actions (8)

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

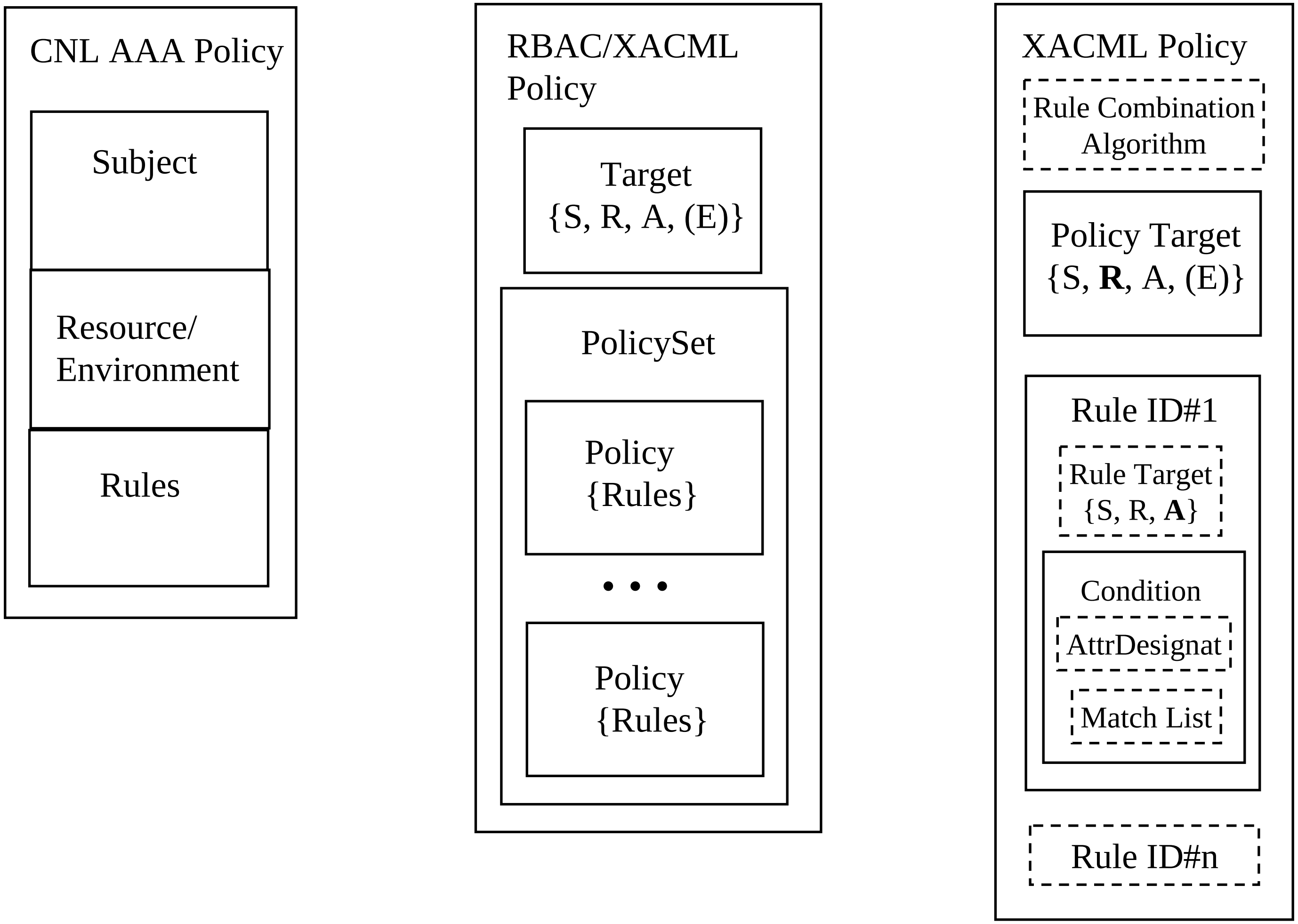
Roles (4)

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

Naming convention

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

Policy formats: AAA and XACML



CNL AAA Policy

Subject

Resource/
Environment

Rules

RBAC/XACML
Policy

Target
{S, R, A, (E)}

PolicySet

Policy
{Rules}

• • •

Policy
{Rules}

XACML Policy

Rule Combination
Algorithm

Policy Target
{S, **R**, A, (E)}

Rule ID#1

Rule Target
{S, R, **A**}

Condition

AttrDesignat

Match List

Rule ID#n

CNL2 AuthZ policy: RBAC using XACML format

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 validation – is not supported by current XACML functionality
  - TODO: add Function or do validation at/by PEP or Context Handler

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>
```

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
- evaluation is done and decision is provided per resource

Issues in using XACML and SAML for Authorization

XACML issues/problems

- No mechanisms for authenticity and integrity
- No communication protocol specified
- No AuthZ session management
- Policy doesn’t have Subject/Attribute (cryptographic) validation function

SAML issues/problems

- No direct mapping from XACML Authz decision to SAML AuthzStatement
- Full AuthZ Assertion is not elegant

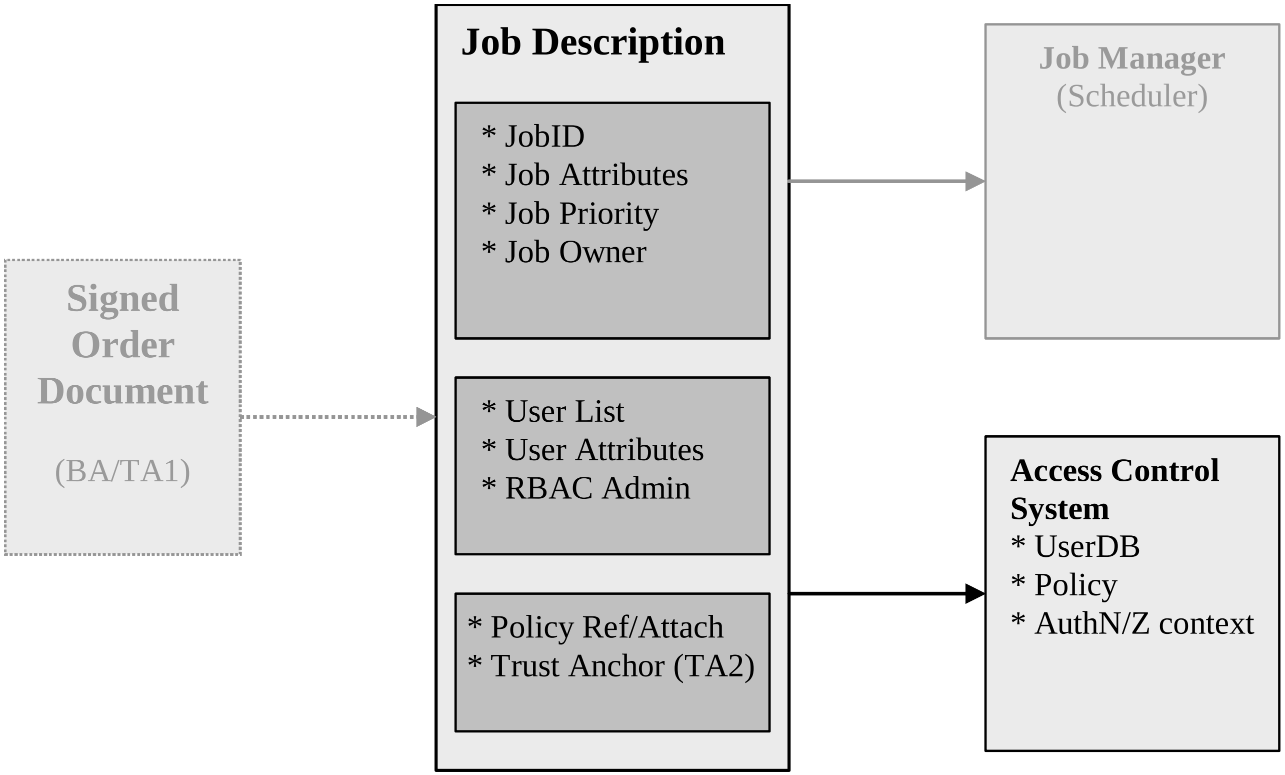
Common SAML and XACML issues

- Complex in implementation
- Require separate key/trust management support
- Require application/community specific attribute namespace definition

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

CNL2 Security built around Job description

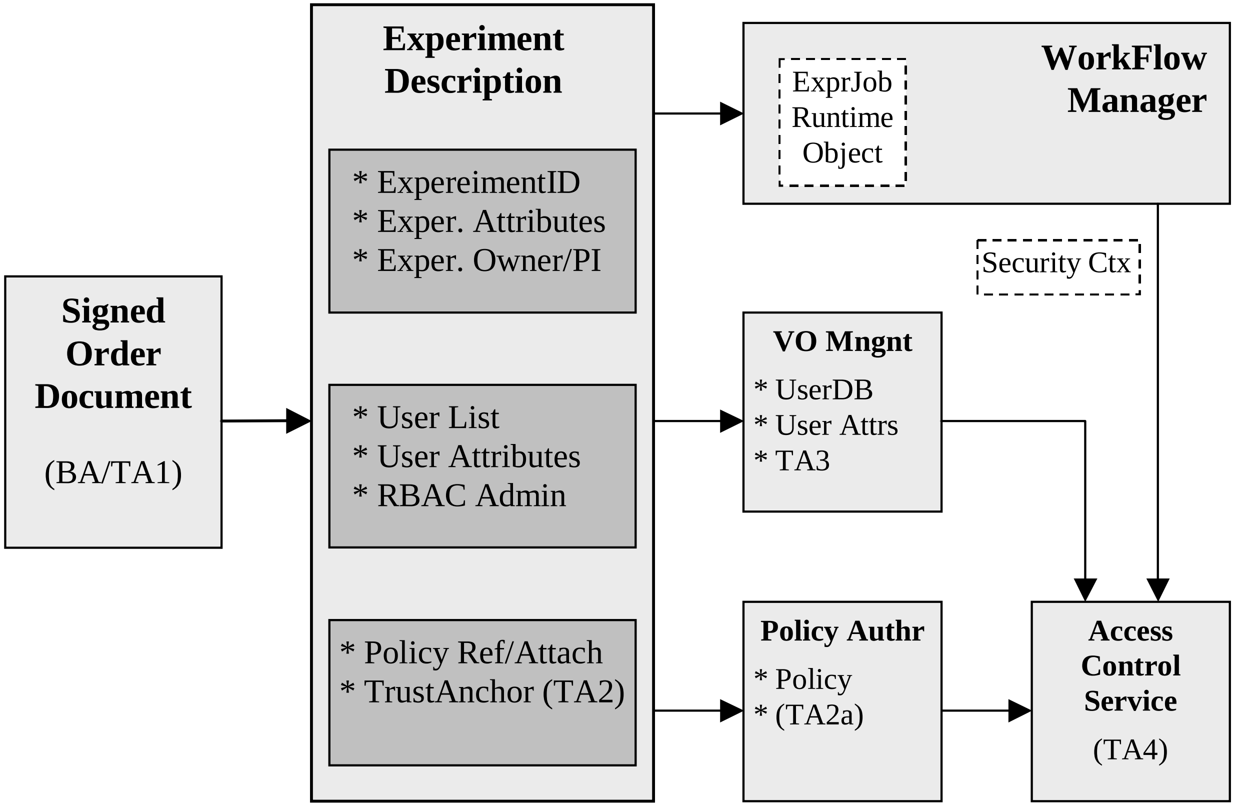


Job Description as a semantic object defining Job attributes and User attributes

- Requires document based or semantic oriented Security paradigm

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

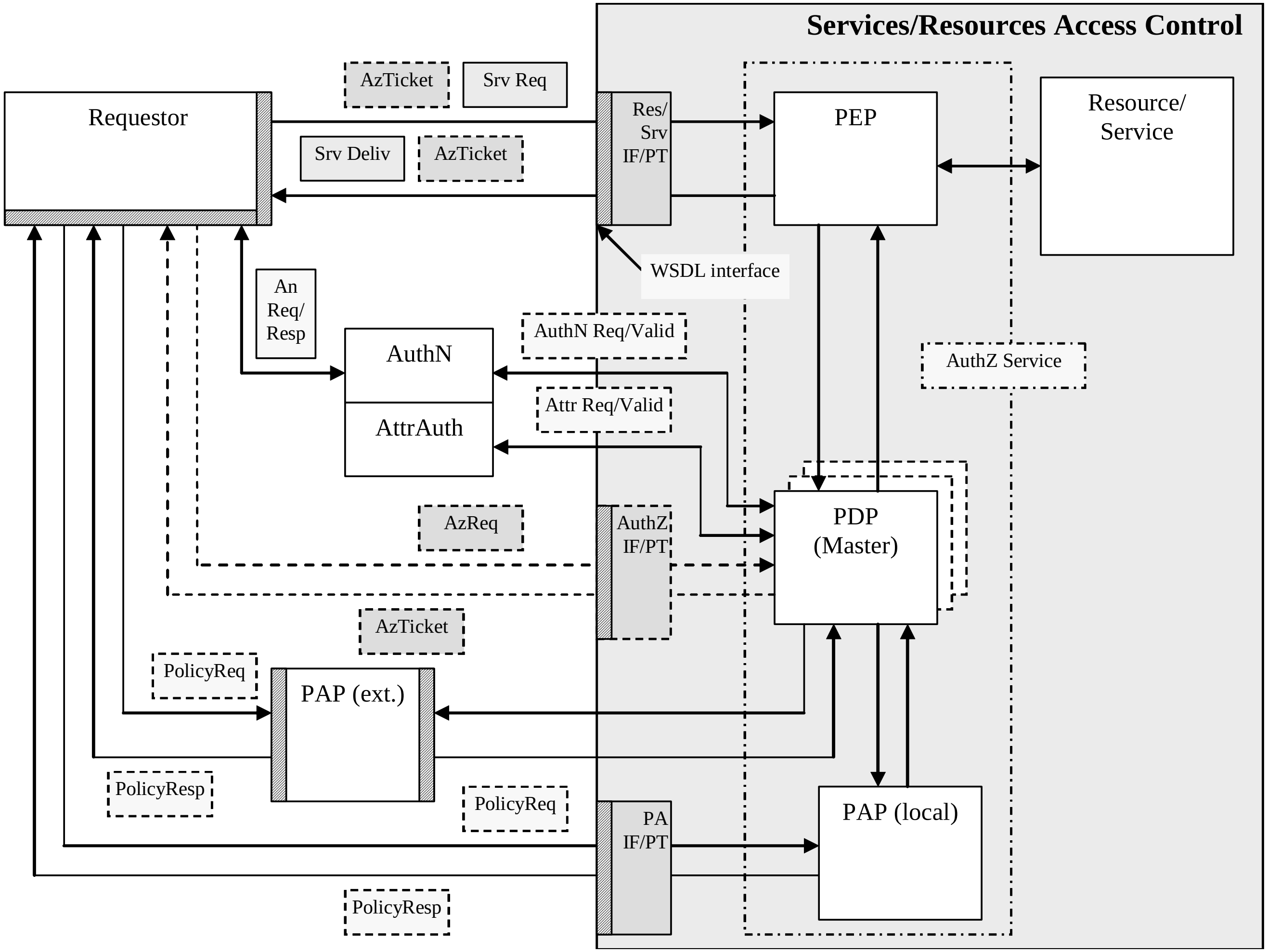
Re-designing to Experiment-centric model in GCE/CNL integrated with the workflow management



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 Agreement (TA)

Moving to Grid/Web Service platform



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

Provides a basis for mutual authorisation

Traditional Access Control model – setting up trust and authority relations

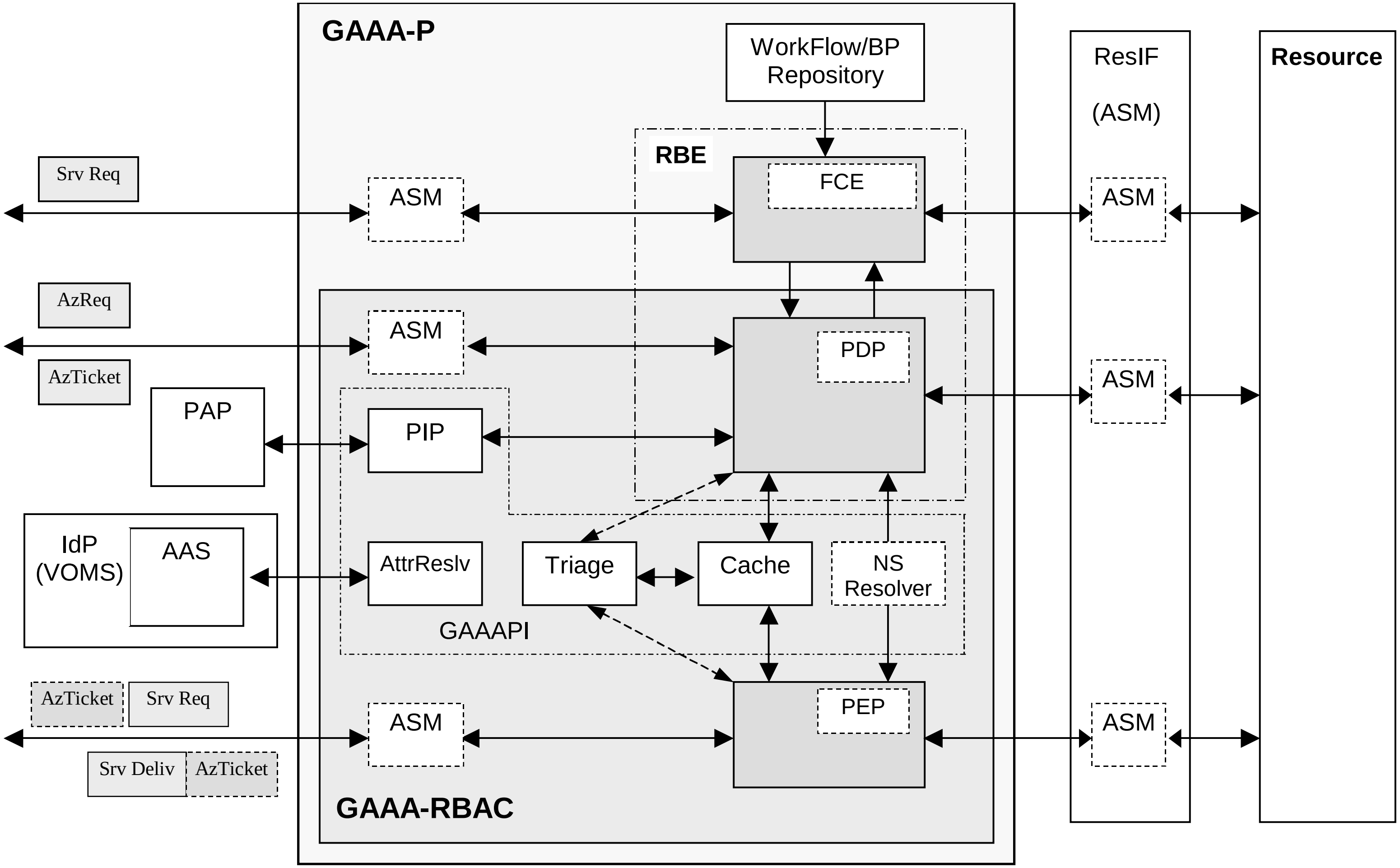
- Policy, attributes semantics and namespaces are known a priory to all participating parties
  - A requestor knows what information to present to adhere to a specific policy and in what format
- PEP and PDP locations are known and interacting parties are known
- Trust relations between PDP, AA and resource are established
  - Resource trusts PDP's decision that can be delivered to a Resource in a form of AuthzTicket or based on default trust between PEP and Resource
  - Root of policy enforcement hierarchy, like in real life, belongs to the resource owner

- This approach is not sufficient for emerging Service Oriented Architecture (SOA) based on Grid and Web Services

Implementation suggestions for GCE/CNL

- PDP and PAP must share common namespace
- Policy and respectively PAP should be referenced in the request message explicitly or known to PEP and PDP a priory
- Every PEP in the chain of policy enforcement should take care of the whole request evaluation/enforcement by calling to a single (master) PDP.
  - PEP should not do multiple decision combination.
- Only one PDP should provide a final decision on the whole request
  - However, PEP may have a possibility to request different PDP types based on request semantics/namespace and referred policy
- When using ticket/token based access control model, the PEP should understand and have a possibility to validate the AuthZ ticket issued by trusted PDP
  - The AuthZ ticket should have validity and usage restriction and contain information about the decision and the resource.
- For the further validation of the AuthZ tickets/token, the PEP may cache the ticket locally to speed-up the validation procedure.

GAAA_tk profiles: GAAA-RBAC and GAAA-P



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

GAAA-P and GAAA-RBAC profiles

- Rule Based Engine (RBE) consists of PDP for individual policies evaluation and FCE to control sequence of policies evaluation and 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 and Cache that provide initial evaluation of the request including validity of provided credentials
    - used also for AuthZ tickets/tokens handling and AuthZ session management
  - Attribute resolver and Policy Information Point (PIP) provide resolution and call-outs to related authoritative Policy Authority Points (PAP) and Attribute Authority Service (AAS)

GAAA_tk: Integration with GT4/gLite AuthZ framework

GT4 Authorisation Frameworks 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

gLite security middleware uses the GT4-AuthZ with some specific extensions

- Provides VOMS credentials handing

Suggested GAAA_tk contribution

- Complex XACML policies evaluation
- Authorisation tickets and tokens handling (application/service level)
- 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.

Security Configuration Parameters

Key store location and access

- keystoreType = "JKS"
- keystoreFile = LOCAL_DIR_KEYSTORE + "keystore5cnlsec.jks"
- keystorePass = “********"
- trustedstoreFile = LOCAL_DIR_KEYSTORE_TRUSTED + "keystore5cnltrusted.jks"
- trustedstorePass = “******"

Trusted and local keys/credentials for PEP trust domain (Certs are selfsigned)

- pepprivKalias = "cnl_pep"
- peppubKalias = "cnl_pep"
- pepprivKpass = "Trust:pep"
- pdppubKalias = "cnl_aaapdp"

Trusted sites or authorities

- trustedAuth = "cnl-trust.xml“ // similar to and to be compatible with Shibboleth

AuthzTicket authority

- tickauth = (tickauthPDP | tickauthPEP)

GAAA-RBAC Trust Domains Configuration

Options for trust domains configuration depend 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

Trust domain identifiers:

- TRUSTDOMAIN_PEP = "urn:cnl:trust:pep";
- TRUSTDOMAIN_PDP = "urn:cnl:trust:pdp";
- TRUSTDOMAIN_PEP_PDP = "urn:cnl:trust:pep-pdp";

Authorities identifiers:

- TICKETAUTHORITY_PEP = "urn:cnl:trust:tickauth:pep";
- TICKETAUTHORITY_PDP = "urn:cnl:trust:tickauth:pdp";

Note: Current implementation is in class ConfigTrustDomains for debugging/demo purposes

GAAA-RBAC security related directories configuration

Configuration directories

- LOCAL_DIR_ROOT = ""
- LOCAL_DIR_KEYSTORE_CNLSEC = LOCAL_DIR_ROOT + "data/keystore/cnlsec/"
- LOCAL_DIR_KEYSTORE_TRUSTED = LOCAL_DIR_ROOT + "data/keystore/trusted/"
- LOCAL_DIR_SYMKEYSTORE = LOCAL_DIR_ROOT + "data/keystore/cnlsec/symkeystore/"
- LOCAL_DIR_SCHEMAS = LOCAL_DIR_ROOT + "data/schemas/“

Temporal directory and cache *-> to be re-designed*

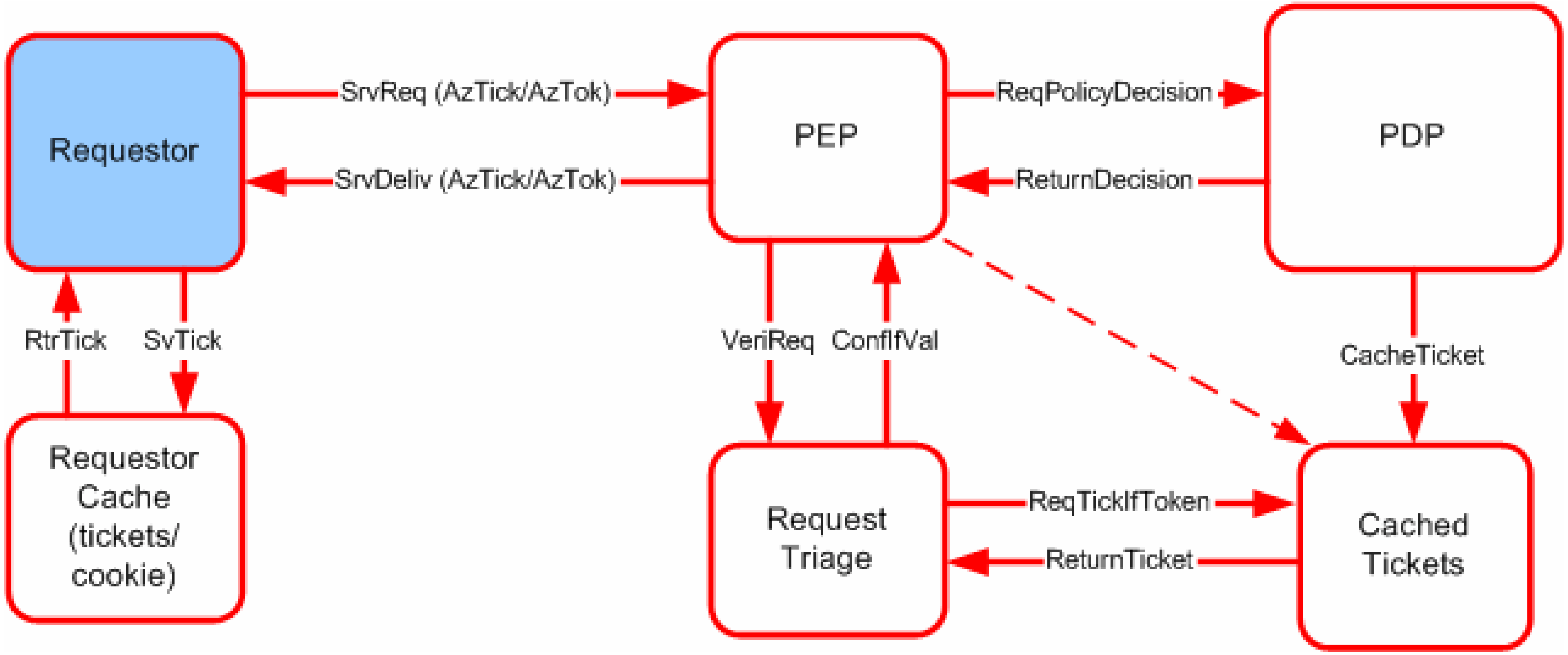
- LOCAL_DIR_AAADATA_CACHE_AZTICKETS = LOCAL_DIR_ROOT + "_aaadata/cache/aztickets/"
- LOCAL_DIR_AAADATA_TMP = LOCAL_DIR_ROOT + "_aaadata/tmp/“

Note. Currently configured in ConfigCNLSecurity class

Session management in GAAA-RBAC

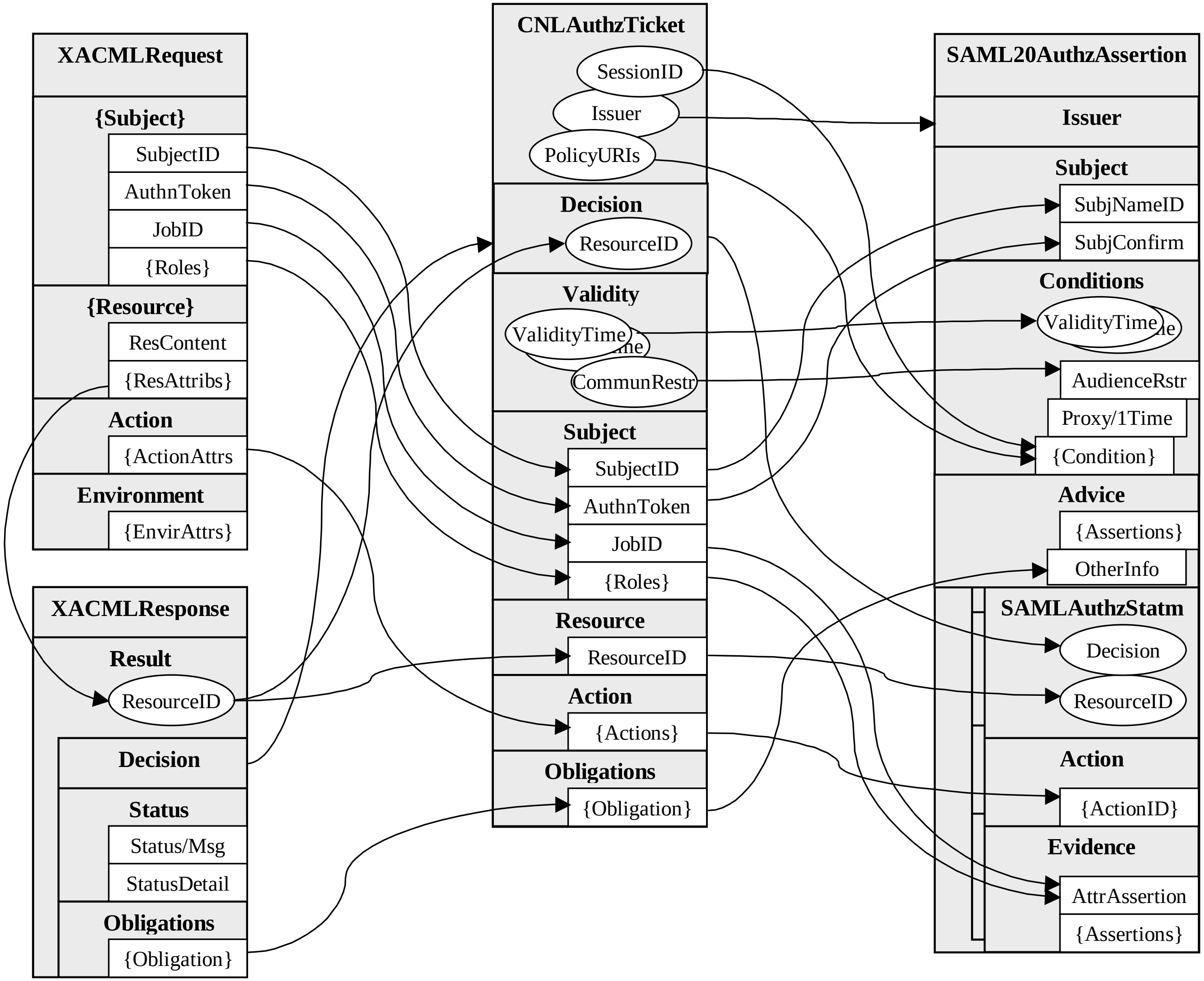
- Maintaining session is a part of generic RBAC functionality
- Session can be started only by authorised Subject/Role
  - Session can be joined by other less privileged users
- SessionID is included into AuthzTicket together with other decision attributes
  - Signed AuthzTicket is cached by PEP or PDP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

Mapping between CNLAuthzTicket, XACML Request/Response and SAML Authorization Assertion



Using SAML 1.1/2.0 for AuthzTicket expression

SAML 2.0 vs SAML 1.1

- Better security features
- Issuer and Subject are top level elements
- Encrypted elements for Subject, Attributes, Evidence
- Special profile for XACMLAuthzStatement
- Support for Identity delegation

General problems for Authorisation assertion

- Attributes can be placed only as deep as 5 level down: **Assertion/AuthzStatement/Evidence/AttributeAssertion/Attribute/AttributeValue**
- Ambiguous location for PolicyURIs and SessionID
- Ambiguous mapping for XACML/Obligation to SAML/(Condition or Advice)
- SAML1.1 ConfirmationData element is an extensible type – compatibility problems
- XACML Obligation element
  - Can be mapped to SAML Condition element or SAML Advice element

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>
```

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 suggests caching CNLAuthzTicket

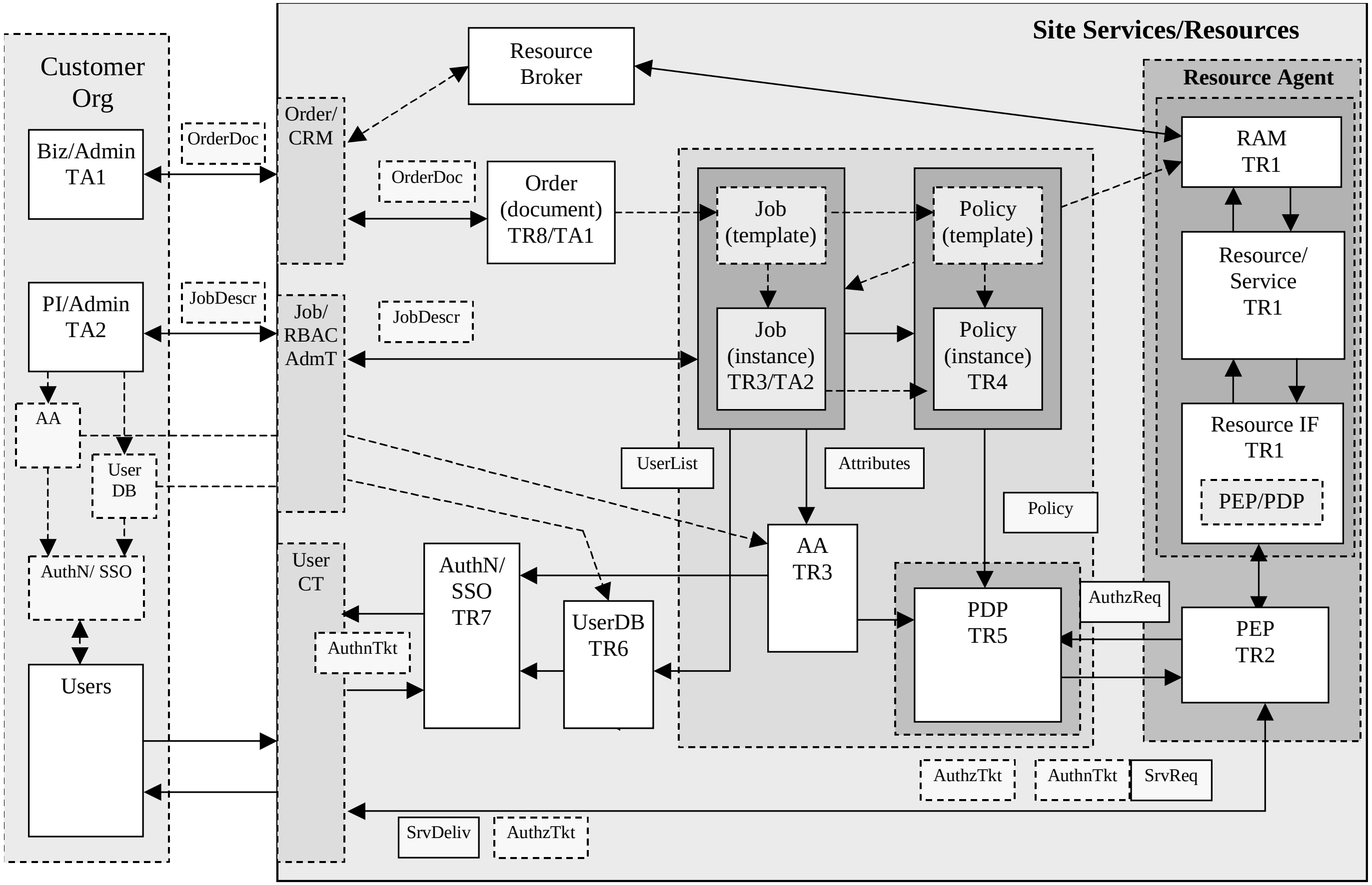
Summary - Future developments

- Common policy expression and evaluation in XACML
  - Provide support for special XACML policy profiles
- GAAA-RBAC/GAAA_tk integration with existing access control tools
  - GT4 Authorization Framework - http://www.globus.org/toolkit/docs/4.0/security/authzframe/
  - (Optionally) EGEE gLite Authorisation Framework - http://glite.web.cern.ch/glite/security/
- Adding support for VOMS credentials – to allow VO-based user and resource attributes management
- Extending GAAA_tk to support different credentials format and callouts

Additional information

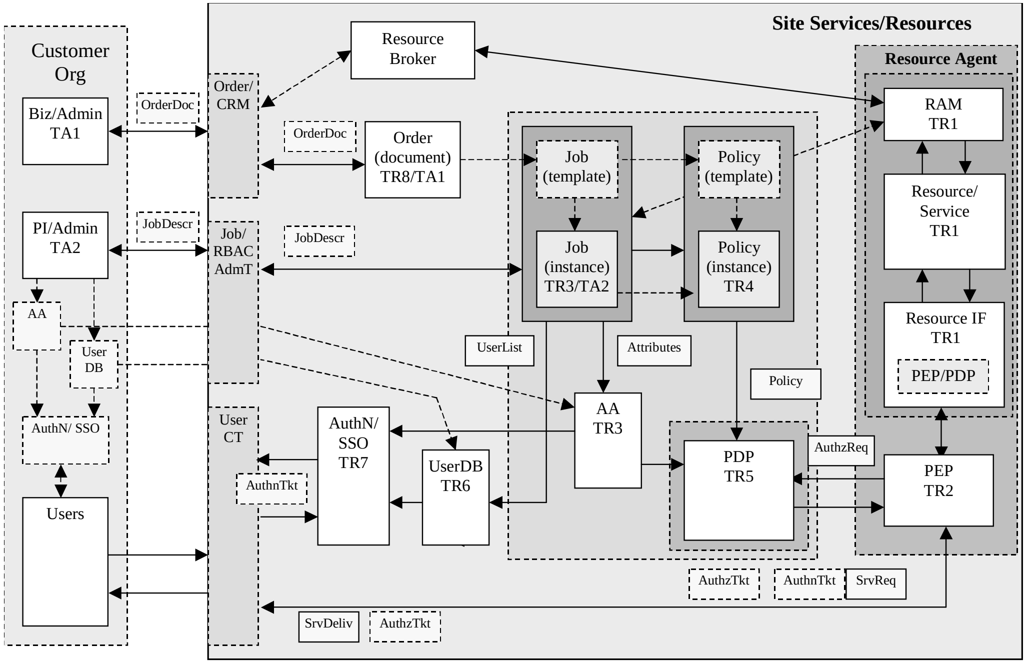
- Generic AAA Architecture and RBAC model
- Interacting components and entities in the Job-centric security model
- XACML AuthZ Request and Response messages format and example
- Detailed AuthZ and AuthN ticket and token examples

Major interacting components and entities in the Job-centric security model



TA – Trust Anchor; TR# - trust path from root (resource); RAM – Resource Allocation and Management; UserCT – User Collaborative Tools

Trust relations in distributed access control infrastructure



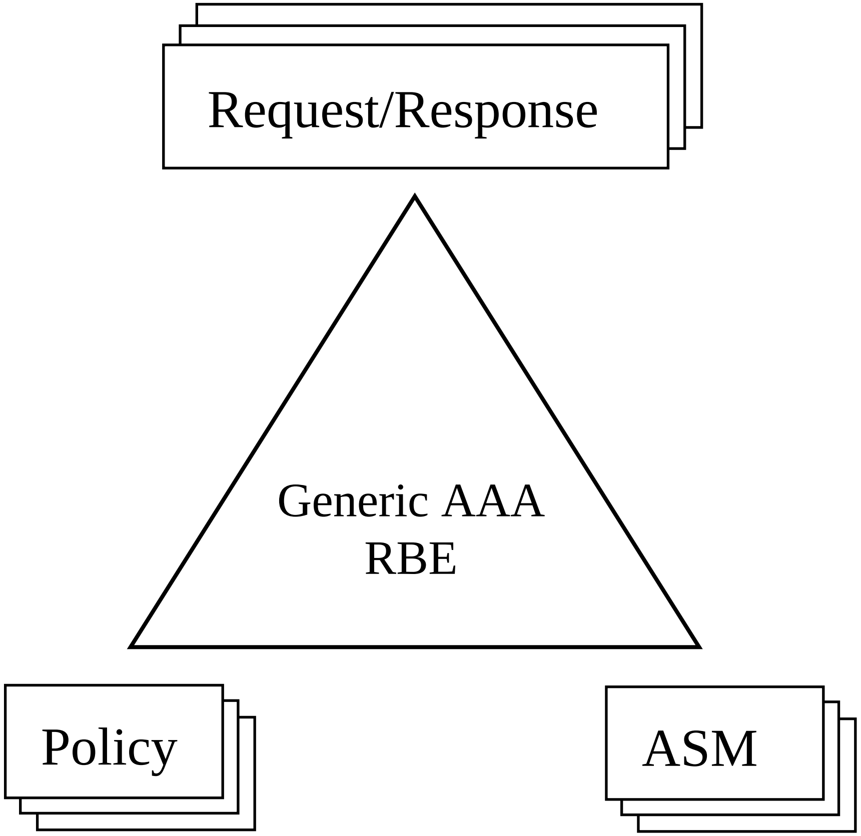
Trust/credentials chain and delegation between major modules:

```
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
```

(1) Generic AAA Architecture by AIRG (UvA)



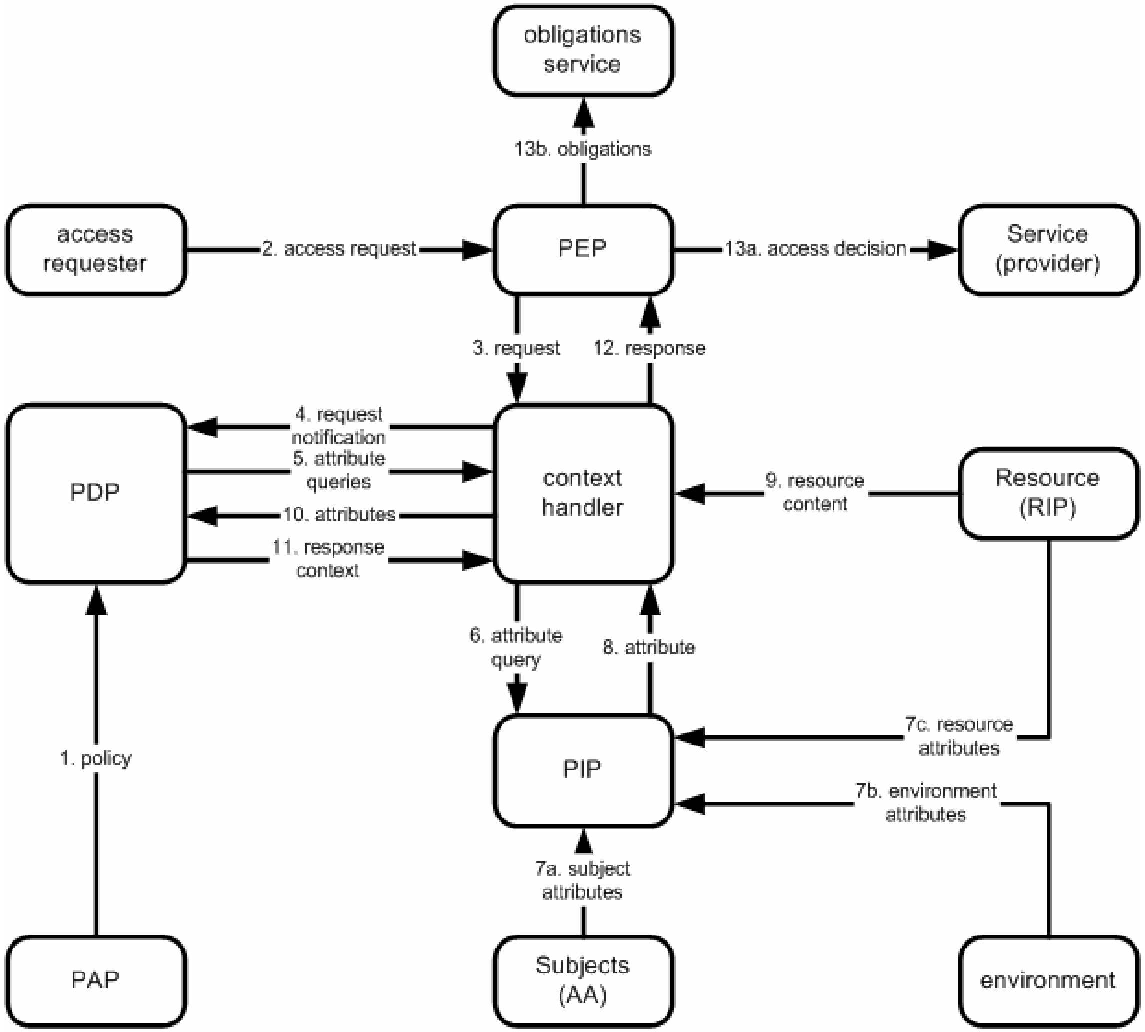
Policy based Authorization decision

- Req {AuthNtoken, Attr/Roles, PolicyTypeId, ConditionExt}
- RBE (Req + Policy) => => Decision {ResponseAAA, ActionExt}
- ActionExt = {ReqAAAExt, ASMcontrol}
- ResponseAAA = {AckAAA/RejectAAA, ReqAttr, ReqAuthN, BindAAA (Resource, Id/Attr)}

•Defined by Resource owner

•Translate logDecision => Action
•Translate State => LogCondition

(2) RBAC: main components and dataflow – XACML model



PEP/AEF - Policy Enforcement Point (authorisation enforcement function)

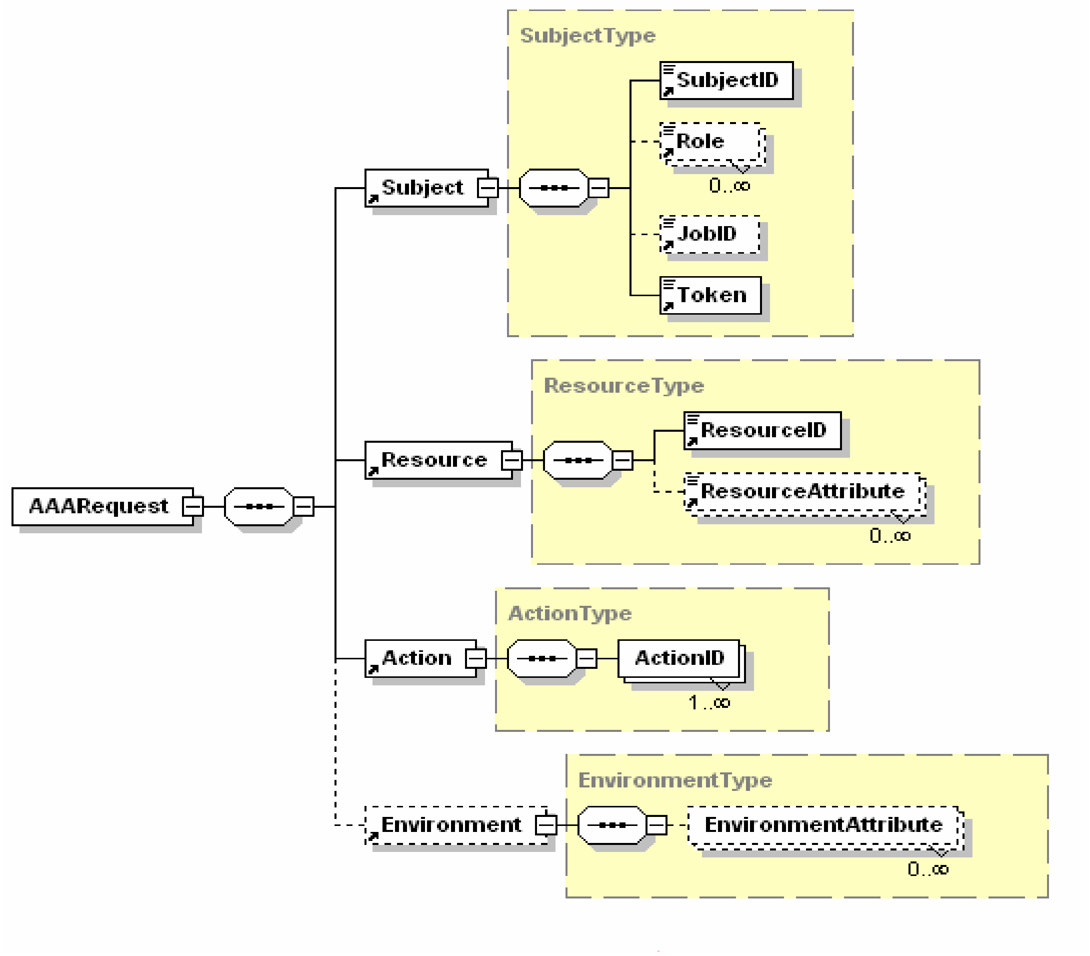
PDP/ADF - Policy Decision Point (authorisation decision function)

PIP - Policy Information Point

AA - Attribute Authority

PAP - Policy Authority Point

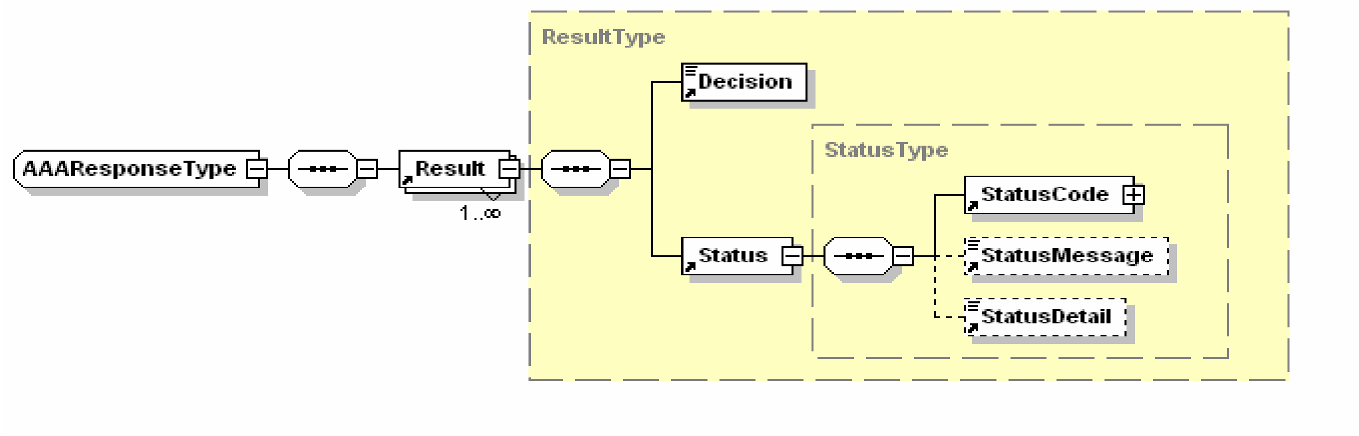
GAAAPI implementation – XACML Request message format



```
<?xml version="1.0" encoding="UTF-8"?>
<AAA:AAARequest
    xmlns:AAA="http://www.AAA.org/ns/AAA_BoD
    "
    xsi:schemaLocation="http://www.AAA.org/n
    s/AAA_BoD
    http://146.50.22.64/CNLdemo1.xsd"
    version="0.1" type="CNLdemo1">
  <Subject>
    <SubjectID>
    WHO740@users.collaboratory.nl</SubjectID
    >
    <Token>
    2SeDFGVHYTY83ZXxEdsweOP8Iok)yGHxVfHom90
    </Token>
   <JobID>JobID-XPS1-212</JobID>
   <Role>Analyst@JobID</Role>
  </Subject>
  <Resource>
    <ResourceID>
    http://resources.collaboratory.nl/Philli
    ps_XPS1
    </ResourceID>
  </Resource>
  <Action>

    <ActionID>ControlInstrument</AttributeID
    >
  </Action>
</AAA:AAARequest>
```

GAAAPI implementation –
XACML Response message format



```
<?xml version="1.0" encoding="UTF-8"?>
<AAA:AAAResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="aaa-cnl-response-00.xsd" version="0.0">
   <Result ResourceId="http://resources.collaboratory.nl/Phillips_XPS1">
         <Decision>Permit</Decision>
         <Status>
                 <StatusCode Value="OK"/>
                 <StatusMessage>Request successful</StatusMessage>
         </Status>
   </Result>
</AAA:AAAResponse>
```

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 suggests 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>
```

CNLAuthnTicket example – 1752 bytes

```
<cnl:CNLAuthnTicket xmlns:AAA="http://www.AAAarch.org/ns/AAA_BoD"
   xmlns:cnl="http://www.aaauthreach.org/ns/#CNL" Issuer="http://www.AAAarch.org/servers/AAA"
   TicketID="f35585dfb51edec48de0c7eadb11c17e">
  <!-- Mandatory elements -->
  <cnl:Validity NotBefore="2005-02-15T14:33:10.548Z" NotOnOrAfter="2005-02-16T14:33:10.548Z"/>
  <cnl:Subject Id="subject">
    <cnl:SubjectID>WHO740@users.collaboratory.nl</cnl:SubjectID>
    <cnl:SubjectConfirmationData>
    0+qQNAVuZW4txMi8DH6DFy7eLMGxSfKDJY6ZnY4UW5Dt0JFtatlEprUtgnjCkzrJUMvWk9qtUzna
    sDdUG+P4ZY7dgab+PHiU91ClusZbztu/ZIjNqCnw5su1BQLTumC8ZTtYKKJi4WWs+bMMbP8mFNQm
    +M7F4bJIPBfLcxf0bk4=
    </cnl:SubjectConfirmationData>
    <!--Optional elements -->
    <cnl:SubjectAttribute attrname="urn:cnl:subject:attribute:job-id">
     CNL2-XPS1-2005-02-02
    </cnl:SubjectAttribute>
    <cnl:SubjectAttribute attrname="urn:cnl:subject:attribute:role">
     analyst@JobID;expert@JobID
    </cnl:SubjectAttribute>
  </cnl:Subject>
</cnl:CNLAuthnTicket>
```

CNLAuthnToken signed/encrypted – 401/269 bytes

```
<cnl:CNLAuthnToken xmlns:cnl="http://www.aaauthreach.org/ns/#CNL"
   TokenID="f35585dfb51edec48de0c7eadb11c17e">
  <cnl:SubjectID>WHO740@users.collaboratory.nl</cnl:SubjectID>
  <cnl:TokenValue>
   0+qQNAVuZW4txMi8DH6DFy7eLMGxSfKDJY6ZnY4UW5Dt0JFtatlEprUtgnjCkzrJUMvWk9qtUzna
   sDdUG+P4ZY7dgab+PHiU91ClusZbztu/ZIjNqCnw5su1BQLTumC8ZTtYKKJi4WWs+bMMbP8mFNQm
   +M7F4bJIPBfLcxf0bk4=</cnl:TokenValue>
</cnl:CNLAuthnToken>
```

- CNLAuthnToken is constructed of the CNLAuthnTicket TicketID and SubjectConfirmationData which is encrypted SubjectID value
- CNLAuthzToken must be self-sufficient and doesn’t require caching CNLAuthnTicket’s

```
<cnl:CNLAuthnToken xmlns:cnl="http://www.aaauthreach.org/ns/#CNL"
   TokenID="a392a20157698d201d77b2c6e8e444ef">
<cnl:SubjectID>WHO740@users.collaboratory.nl</cnl:SubjectID>
<cnl:TokenValue>qij9zJgKZp9RiJxYN1QJAN0vhjLJSMGVLD/doQtmCsk=</cnl:TokenValue>
</cnl:CNLAuthnToken>
```