Extending GAAA-RBAC for Dynamic Grid-based Collaborative Environment

Yuri Demchenko <demch@science.uva.nl>

System and Network Engineering Group

University of Amsterdam

Outline

- Background – basic use cases and target projects
- GAAA-RBAC functionality for CNL3 domain based architecture
- GAAA-RBAC profile – design and implementation suggestions
  - ◆ Configuration and trust domains management
  - ◆ Using AuthZ tickets and tokens for performance optimisation and AuthZ session management
    - – DEMO
  - ◆ Role Based Access Control (RBAC) and XACML policy examples
    - – DEMO
- Summary – Future development
- Additional materials (technical)

GAAA – Generic Authentication, Authorization, Accounting

GAAA-AuthZ – GAAA AuthZ Framework

Background – basic use cases and target projects

- Central Authorisation service for Collaboratory.nl project
  - Architecture, Framework and Implementation
- Distributed multidomain Authorisation service for OLPP (RoN GP-NG)
  - Gap analysis produced
- (planned) LUCIFER Service plane AAA-AuthZ focused toward multi-domain optical networking
- (negotiated) EGEE migration from gLite-AuthZ to GT4-AuthZ

Stages/Evolution

- Adopting GAAA_tk for CNL1 AuthZ service – CNL1 (2003-2004)
- GAAAPI for simple local policy and GAAA_tk callout – CNL2 (2004-2005)
- GAAA-RBAC profile designed for CNL3 (2005-2006)
  - To be compatible with (and orthogonal to) to GT4-AuthZ and prosp. Acegi

CNL3 Overview - Used technologies and development platform

- GridSphere Portal (JSR-168 portlet std compliant)
  - Create virtual working environment
  - Manage Instrument
  - Extension by writing own portlets
- Eclipse Rich Client Platform (RCP)
  - Extensive range of plugins and libraries for collaborative applications
    - chart, whiteboard, videostreaming, etc.
  - Rapidly developing platform
- Acegi security for Spring/J2EE as a framework for integrating applications and security services
  - Interceptor service plugins/callouts (aspect-oriented programming)
    - Currently used simple ACL
    - Potential extensibility with advanced AuthZ modules, e.g. GAAA-AuthZ

CNL3 domain model – Resource hierarchy and services context

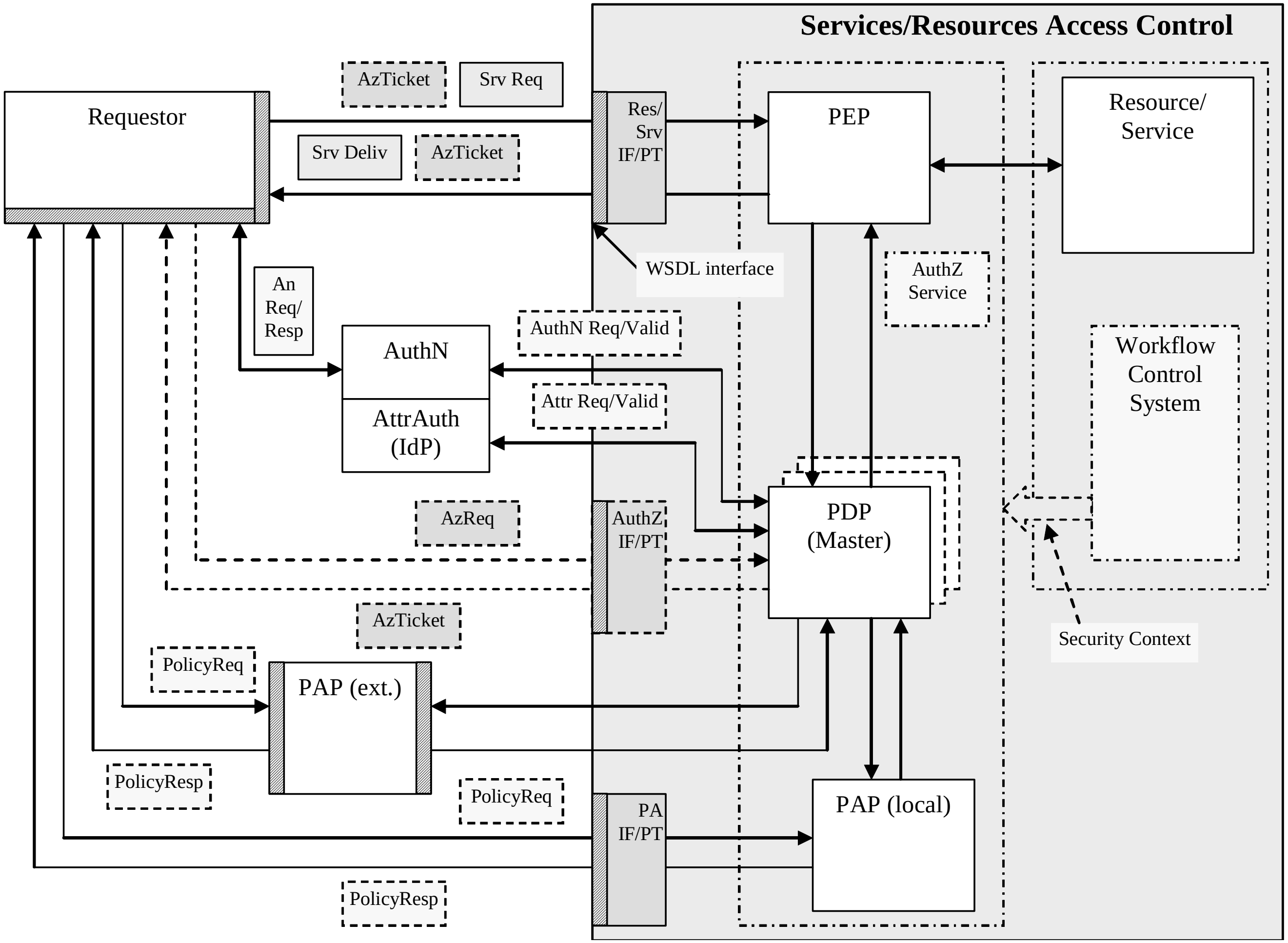
Facility > Virtual Lab > Experiment > Experiment/Collaborative Session

- Provides context for
  - Instrument as the access object Resource
  - User roles/attributes
- Users as registered users at hosted Facility or member Facility

Two solutions/mechanisms to flexibly manage security context

- Experiment workflow
- Context aware Access control infrastructure

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

Security context management: Changing information and mechanisms

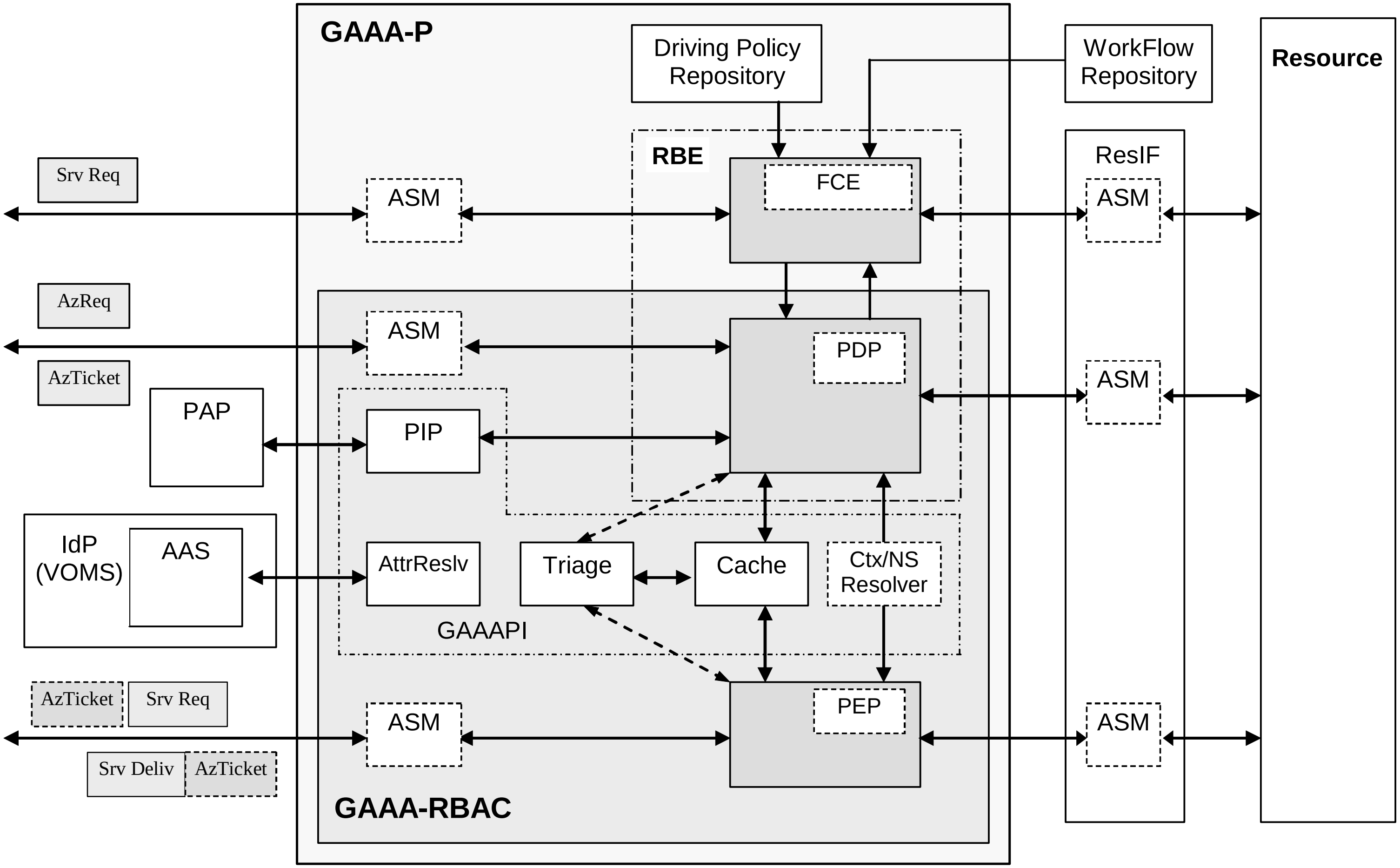
Context dependent information/attributes:

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

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-RBAC/GAAAPI Security Configuration

General security configuration

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

Trust domains and authorities

- 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
- AuthzTicket authority (tickauthPDP | tickauthPEP)

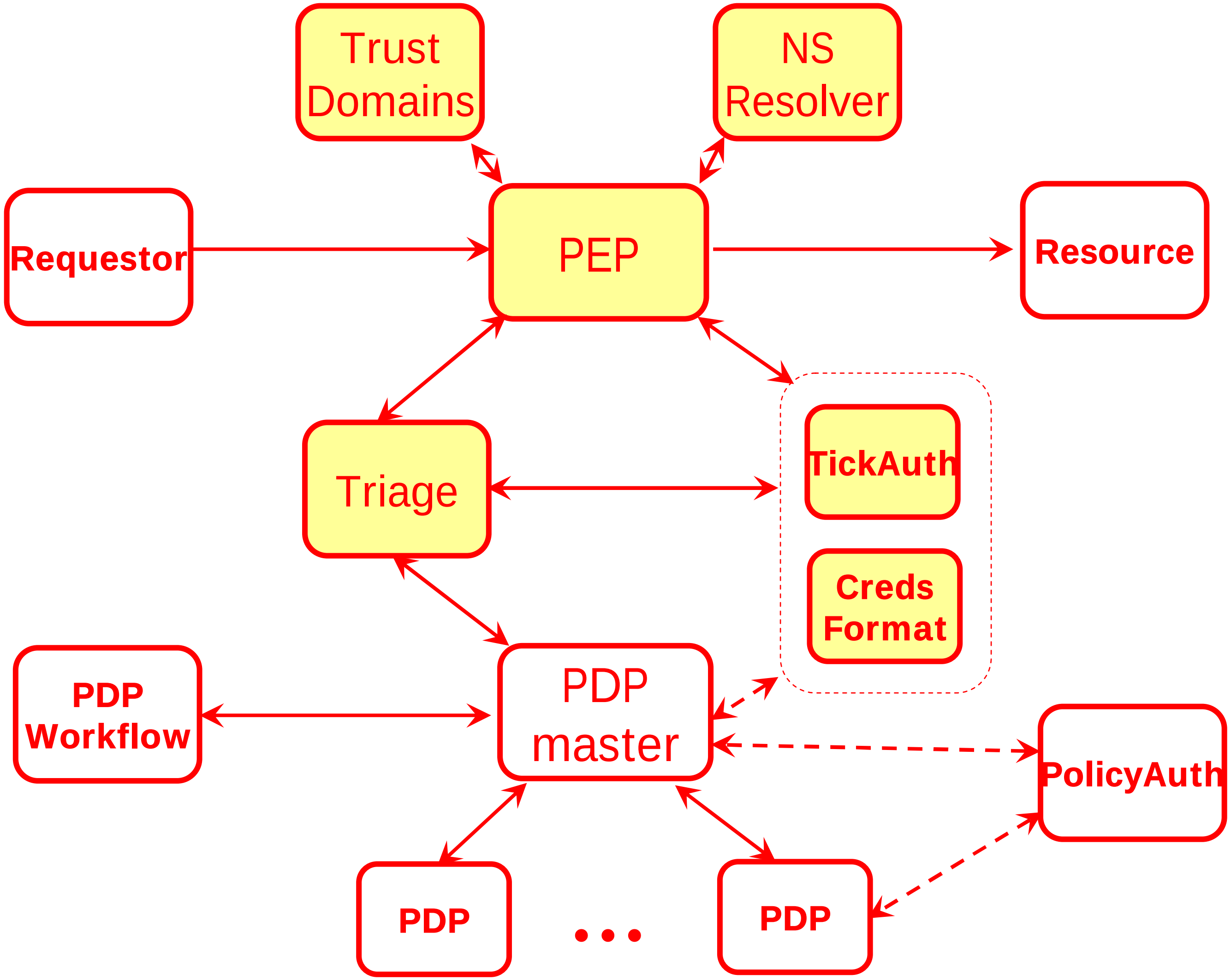
PDP Configuration

- Standard XACML PDP configuration => master PDP configuration with components and evaluation flow

PEP Configuration

- Namespace Resolver
- Ticket Authority
- Trust domains
- Session credentials or exchange ticket/tokens format

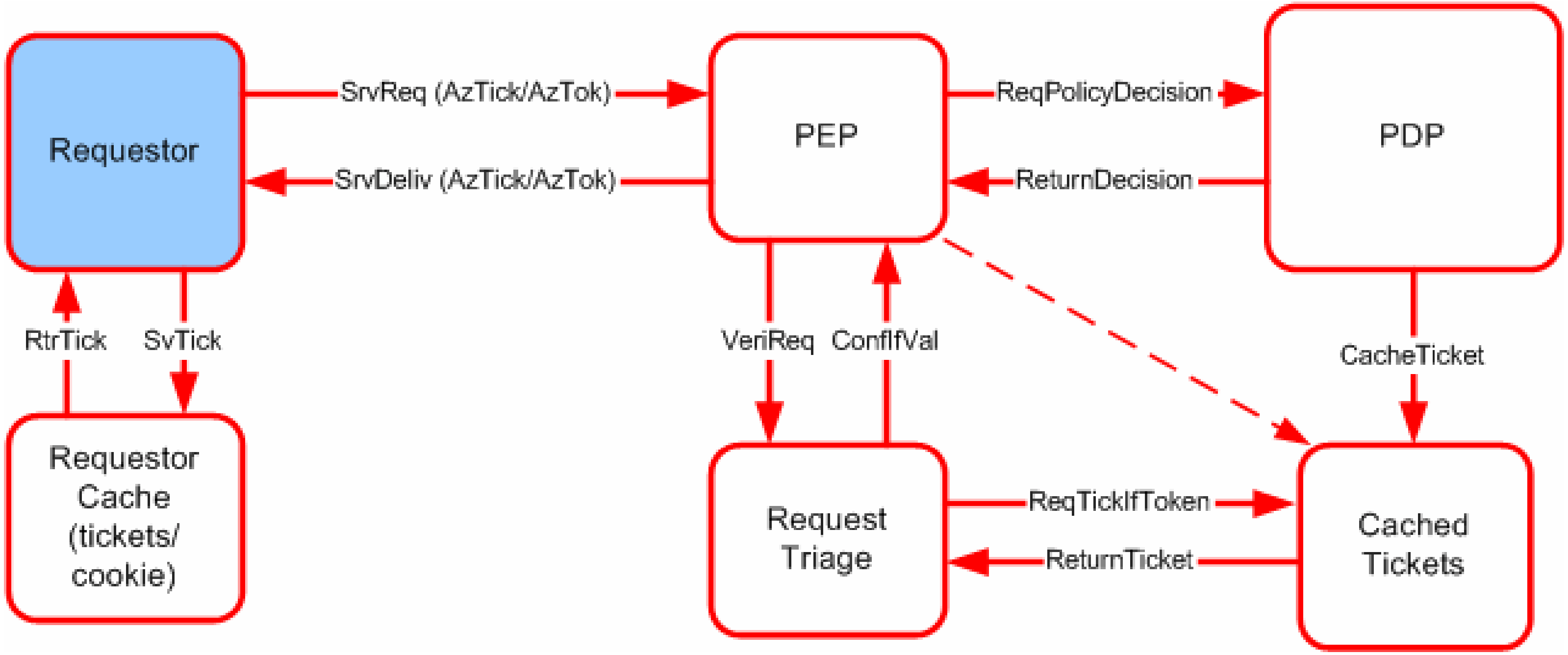
PEP Configuration components



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

GAAA AuthzTicket format

```
<cnl:CNLAuthzTicket xmlns:AAA="" xmlns:cnl="http://www.aaauthreach.org/ns/#CNL"
   Issuer="urn:cnl:trust:tickauth:pep" PolicyURIs="CNL2policy01-test"
   SessionIndex="sessionID-2005-03-23-test" TicketID="e916c88a86462d0e26cd4faae1de88ae">

   <cnl:Decision ResourceID="Phillips_XPS1">Permit</cnl:Decision>

   <cnl:Validity NotBefore="" NotOnOrAfter="2006-05-09T10:17:28.646Z"/>

   <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-XPS1-2005-02-02</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>
```

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

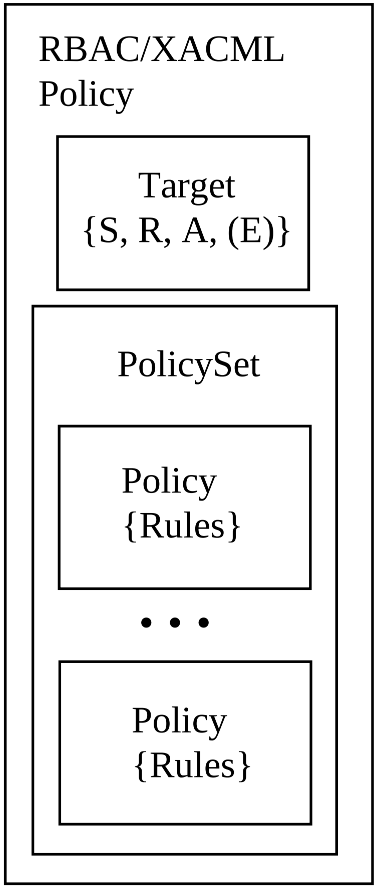
```
<cnl:CNLAuthzToken TokenID="c24d2c7dba476041b7853e63689193ad">
<cnl:TokenValue>
0IZt9WsJT6an+tIxhhTPtiztDpZ+iynx7K7X2Cxd2iBwCUTQ0n61Szv81DKllWsq75IsHfusnm56
zT3fhKU1zEUsob7p6oMLM7hb42+vjfvNeJu2roknhIDzruMrr6hMDsIfaotURepu7QCT0sADm9If
X89Et55EkSE9oE9qBD8=
</cnl:TokenValue>
</cnl:CNLAuthzToken>
```

- CNLAuthzToken is constructed of the CNLAuthzTicket TicketID and SignatureValue
- CNLAuthzToken use suggests caching CNLAuthzTicket

Demo – AuthZ Tickets/Token handling

DEMO - XACML Policy generation

XACML Policy format



RBAC/XACML Policy

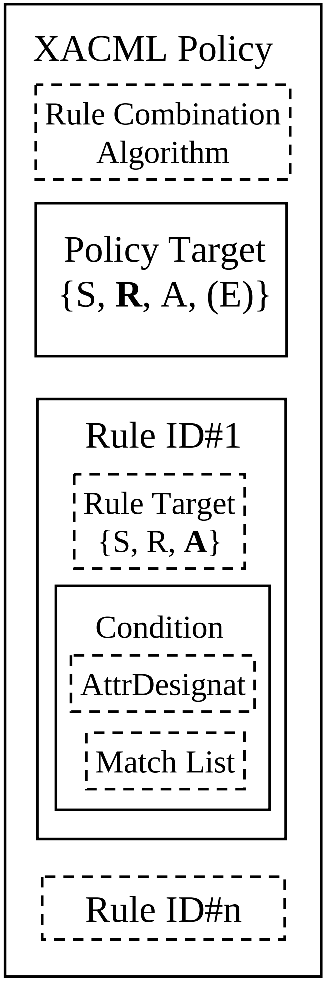
Target {S, R, A, (E)}

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

CNL3 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

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@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>
```

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/PDP 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

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

Demo – Simple XACML Policy generation

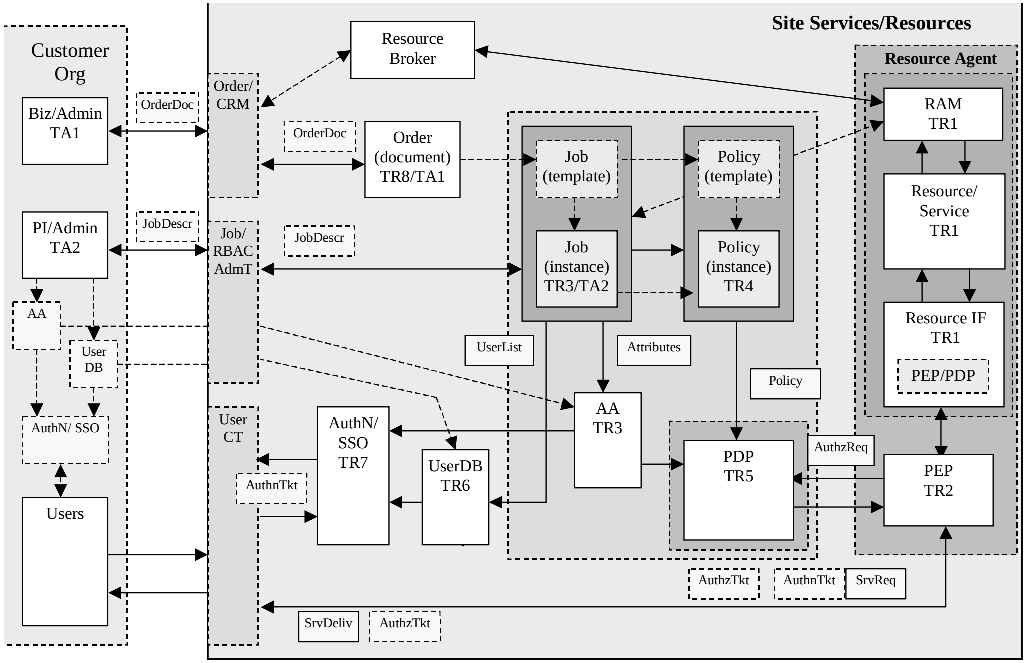
Summary and Future developments

- Integration with existing access control tools
  - GT4 Authorization Framework
  - GT4-AuthZ adoption in EGEE gLite
  - 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 Demo
  - Contribution to CNL domain security model

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

Trust relations in distributed access control infrastructure



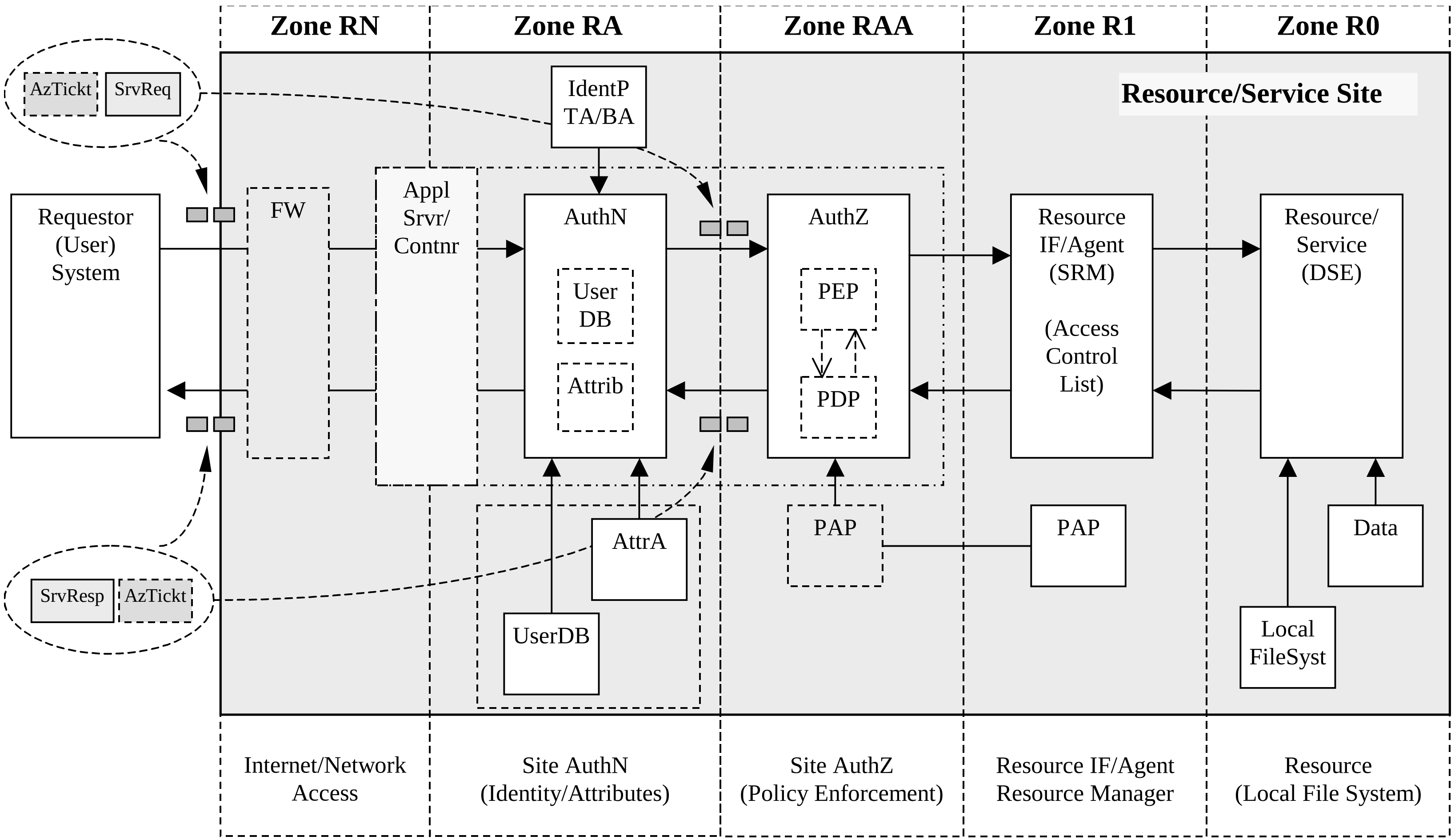
Trust/credentials chain and delegation between major modules:

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

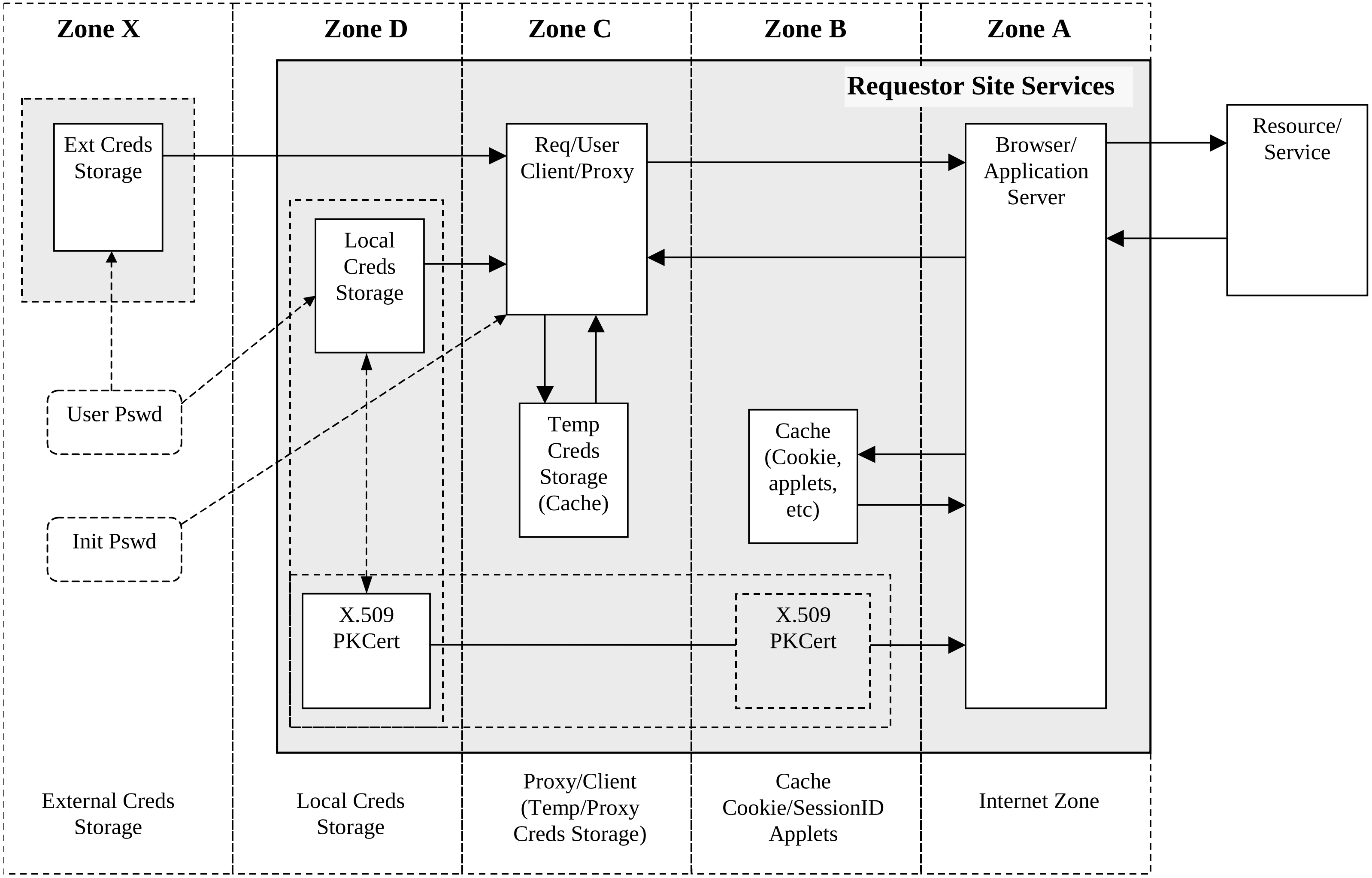
Obtaining required permissions to perform requested action by the user:

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

Resource Zone Security model for Grid/Web Services



Requestor Zone Security model for Grid/Web Services



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>
```