GAAA Authorisation Framework
for Collaborative Applications

virtual laboratory for e-science

Yuri Demchenko
<demch@science.uva.nl>
AIRG, University of Amsterdam

This work is funded by Collaboratory.nl, the EU project EGEE and GigaPort

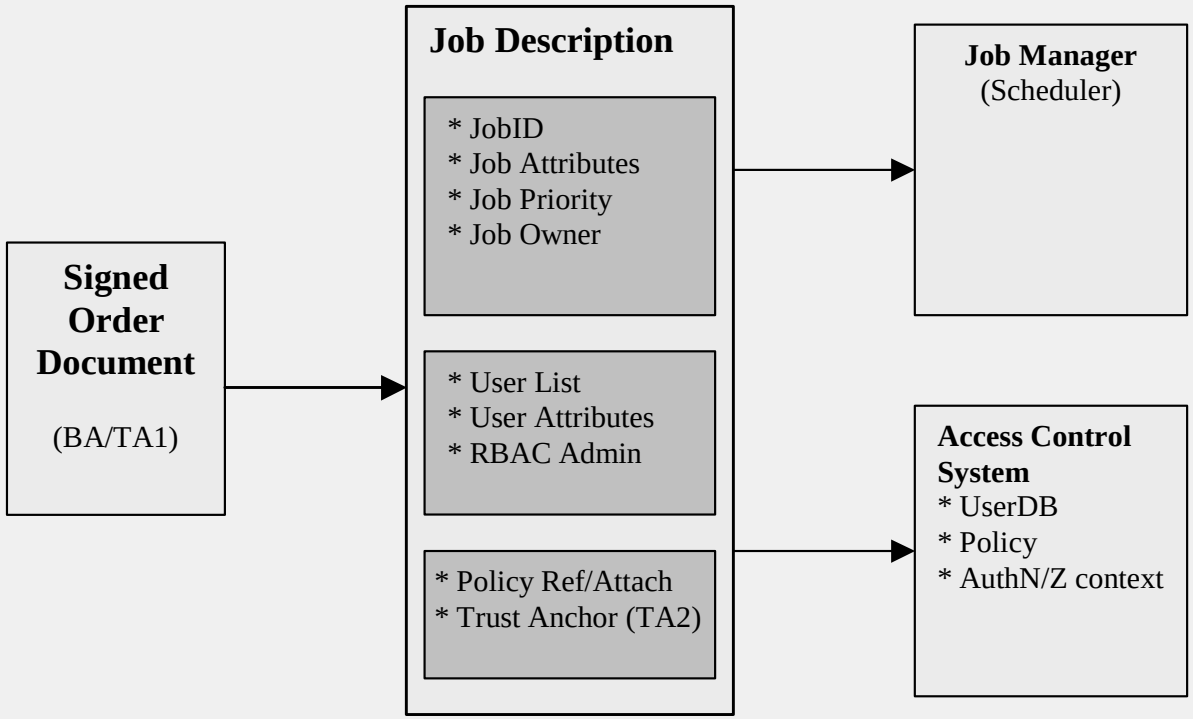
Outline

- ✓ Security requirements to Open Collaborative Environment (OCE)
- ✓ Job-centric security model for OCE Security Architecture
- ✓ Using Generic AAA Authorisation framework and Role Based Access Control (RBAC) for fine grained access control
  - Optimised push-pull-agent model using AuthZ tickets and tokens
- ✓ GAAAPI and implementation details – Collaboratory.nl project
- ✓ Summary - Used technologies and new developments
- ✓ Additional materials (technical)

OCE specific security requirements and common problems

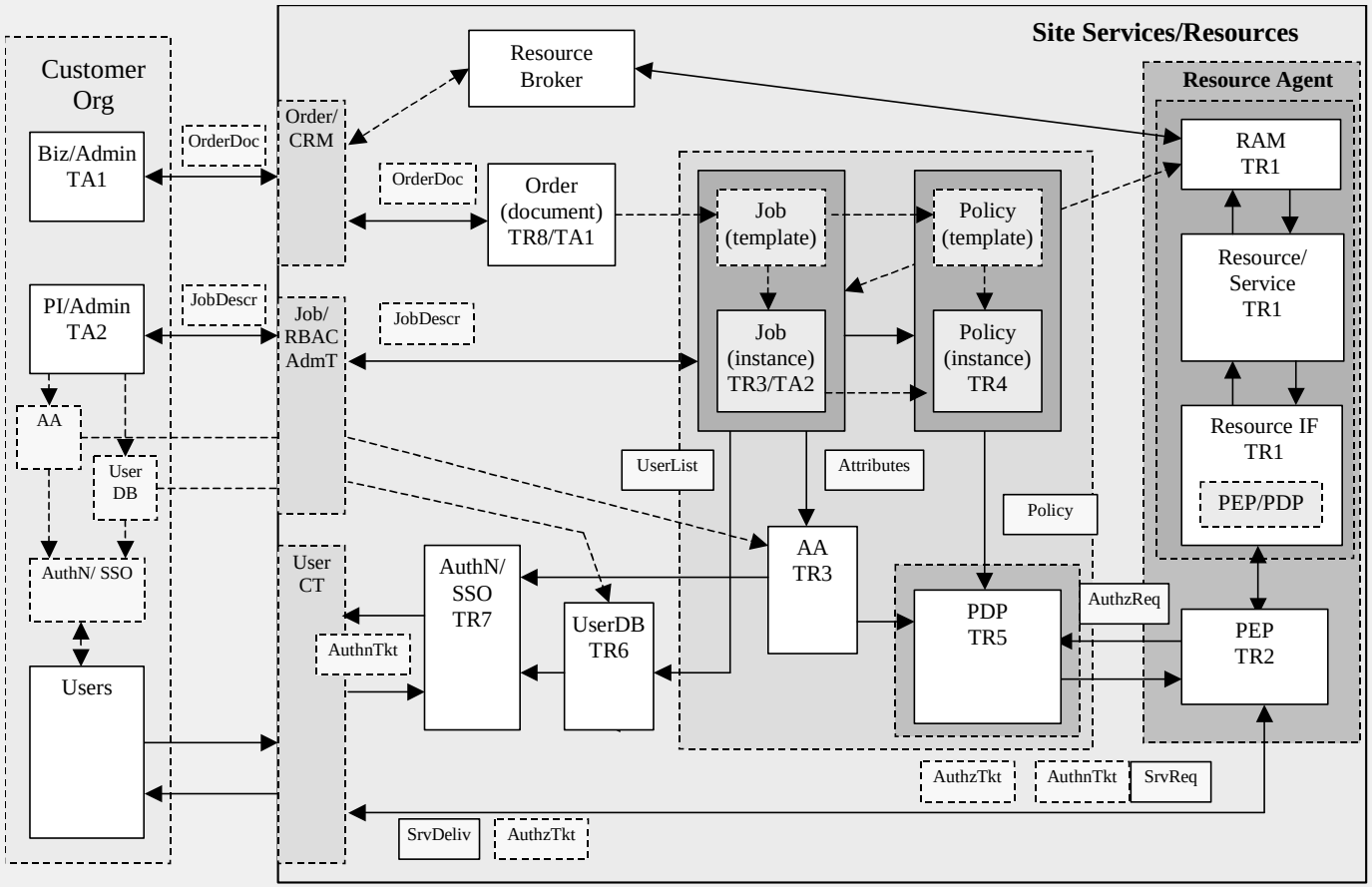
- ✓ Open Collaborative Environment specific security requirements
  - Dynamic and multidomain
  - Customer driven
  - Human controlled and interactive
  - Data protection: personal, experimental data and metadata
- ✓ Common problems addressed
  - Authorisation service performance
    - ➢ Using XML based ticket/token – integrity and secure context management
  - Key management and trust relations in distributed access control infrastructure
  - Compatibility and integration with existing access control tools
    - ➢ Policy formats mapping for flexible policy exchange and combination

OCE/ CNL Security built around Job description



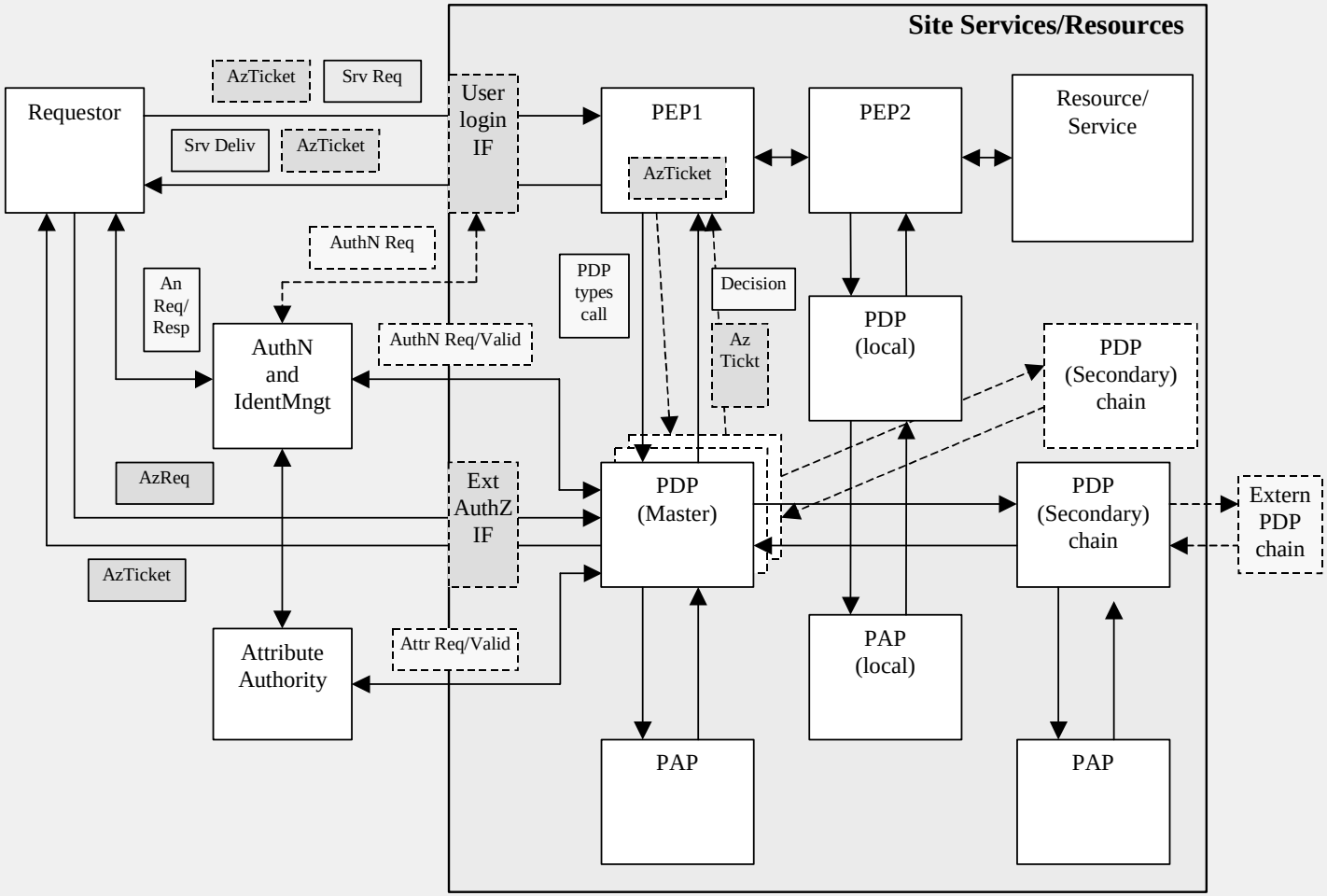
- Job Description as a semantic object defining Job attributes and User attributes
  - ✓ Requires document based or semantic oriented Security paradigm
- Trust domain based on Business Agreement (BA) or Trust Agreement (TA) via PKI

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

Site Authorisation service implementing RBAC and combined pull-push model



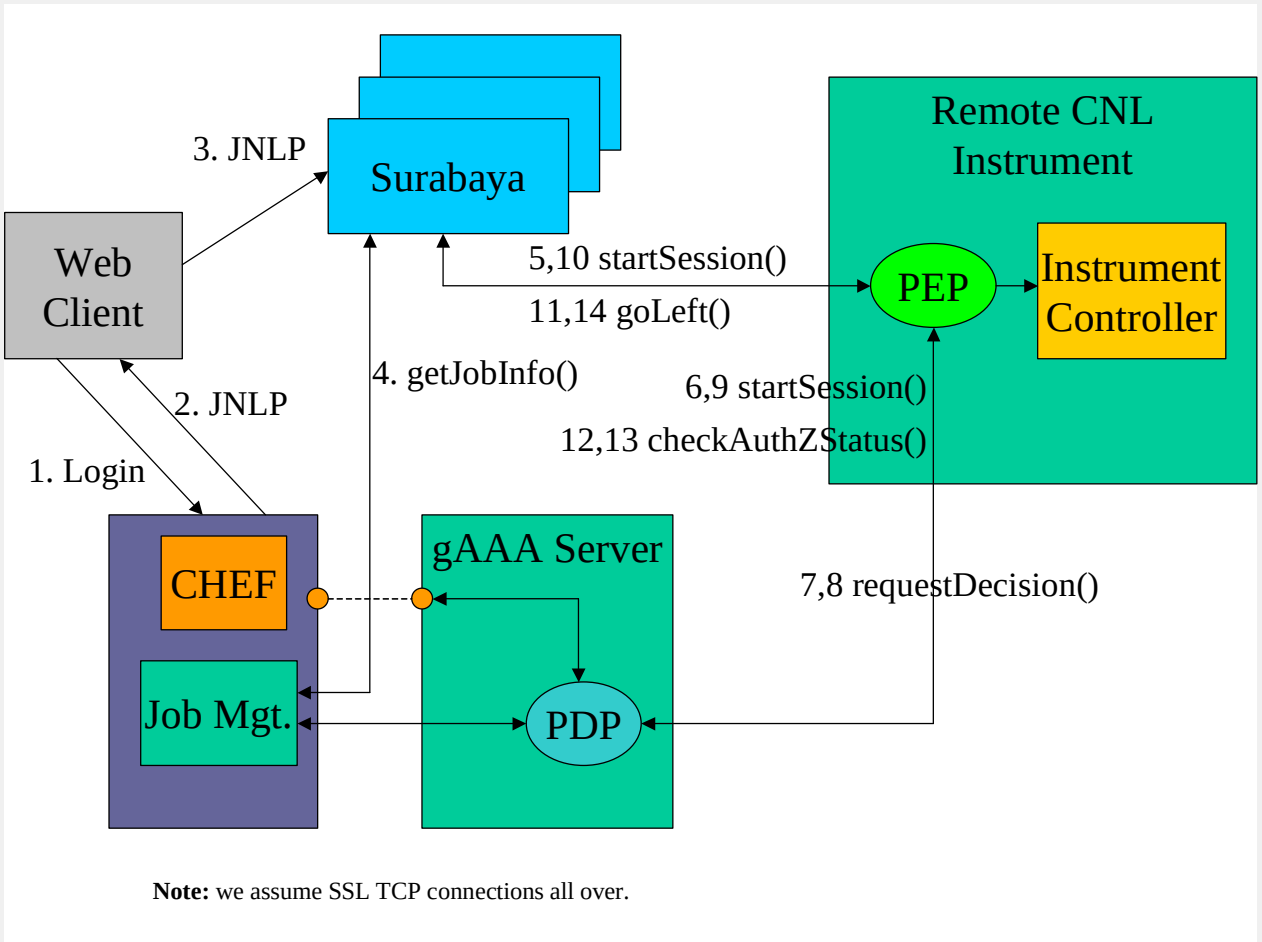
Implementation suggestions for OCE/CNL

- 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.

Before deploying security infrastructure

- 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/tickets format
    - Standard vs proprietary
  - ✓ Protocols and Messages format
    - SOAP + XACML Request/Response
    - SOAP + SAMLP + XACML

Authorisation Service operation in a CNL2 Demo system



JNLP – Java Network Launch Protocol

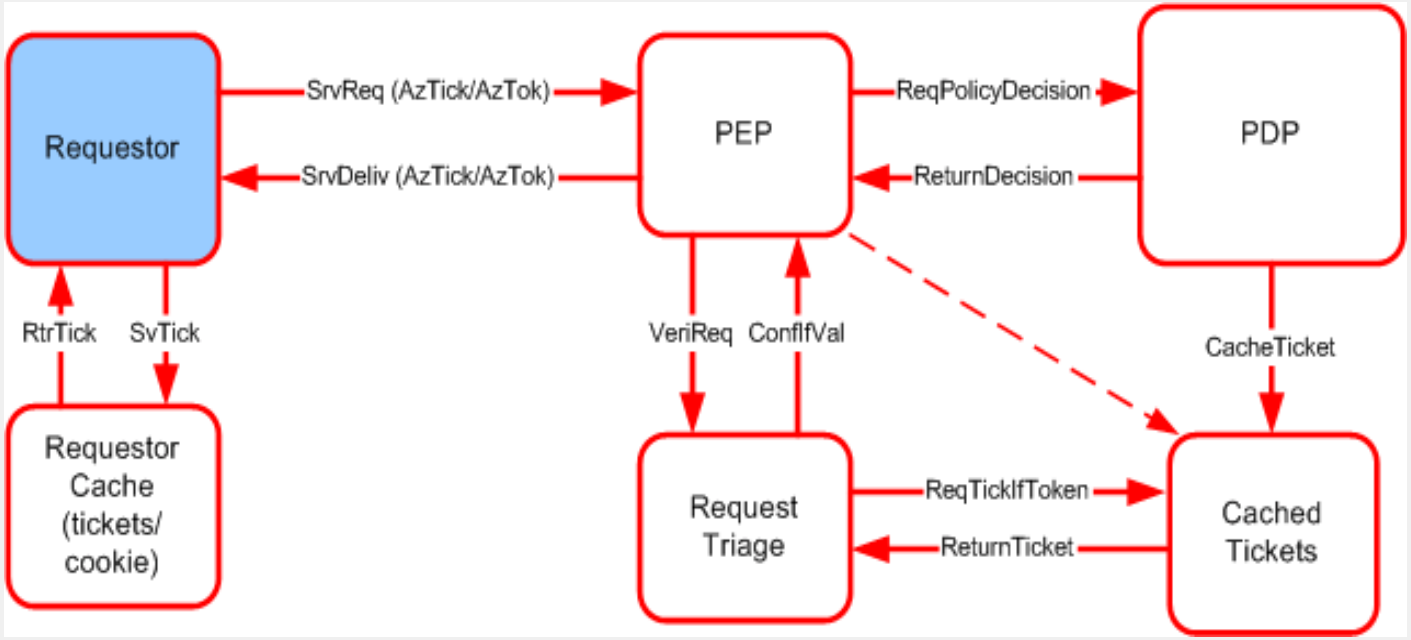
CHEF – Collaborative tool

Surabaya – Collaborative Workspace environment

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”

Tickets/Tokens handling in AuthZ system

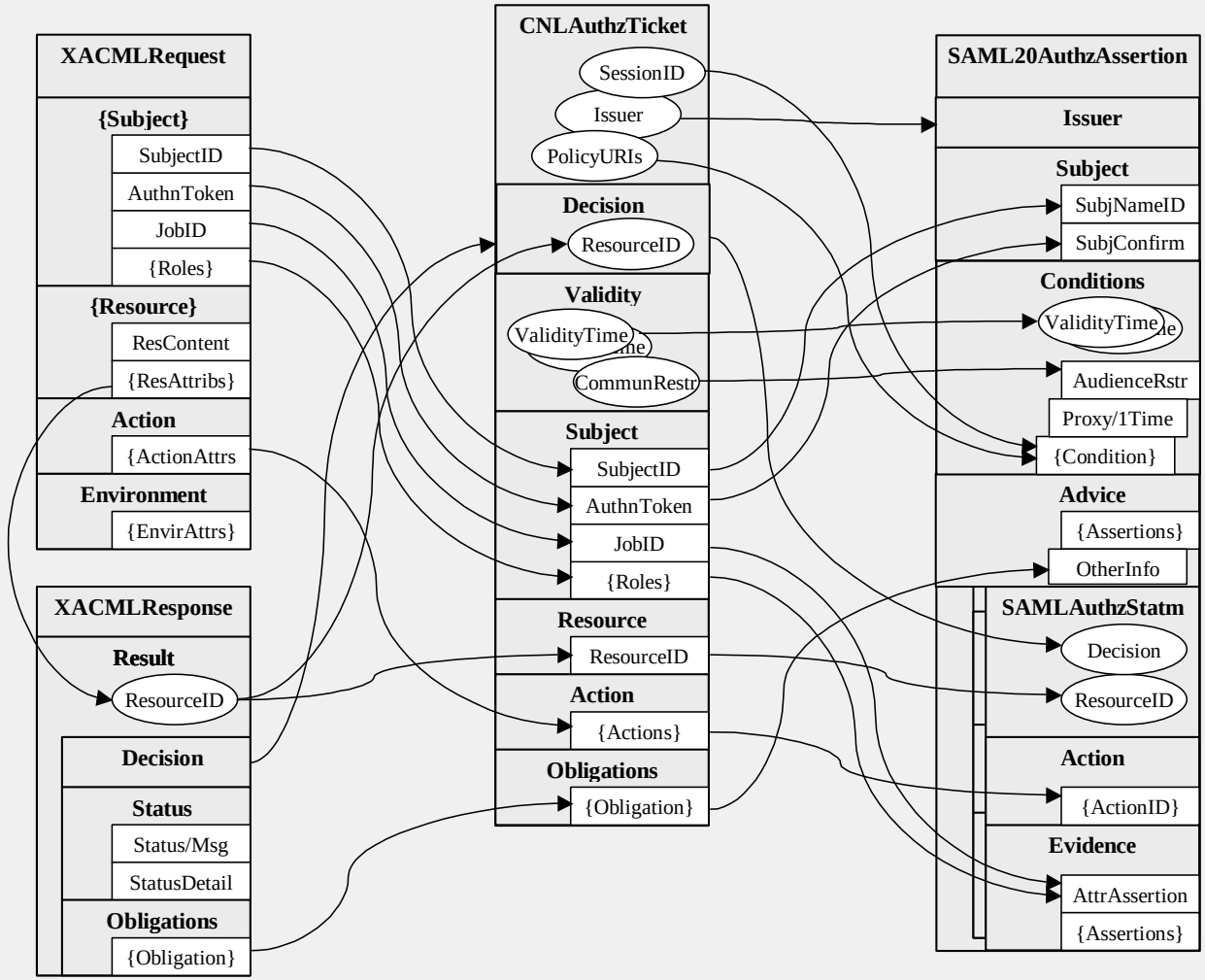


- ✓ AuthzTicket is issued by PDP and may be issued by PEP
- ✓ AuthzTicket must be signed
- ✓ AuthzTicket contains all necessary information to make local PEP-Triage Request verification
- ✓ When using AuthzToken, AuthzTicket must be cached; Resolution mechanism from token to ticket must be provided

Session management in CNL2 AuthZ system

- 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

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

General problems for Authorisation assertion

- Attributes can be placed only as deep as 5 level down: Assertion/AzStatemt/Evidence/AttrAssert/Attr/AttrValue
- Ambiguous location for PolicyURIs and SessionID
- 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="ed9d969e1262ba1d3a7f33dbd670dd94">
<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 - Used technologies and new developments

- ✓ Job-centric security model that responds OCE dynamic distributed requirements
  - Job description format – to be compatible with WS-Agreement and GGF JSDL (Job Submission Description Language)
- ✓ Extended RBAC functionality based on GAAA Authorisation framework
  - AuthZ/Resource Session management
- ✓ GAAA_tk as RBE and AAA policy expression
  - XACML Request/Response messaging
  - Migration to XACML based policy exchange and combination
- ✓ Proprietary and SAML based AuthzTicket format including SAML2.0 extensions
- ✓ XML Signature and XML Encryption for JobDescription and AuthzTicket security
- ✓ Contribution to XACML, SAML and GT4 development

Summary - Future development

- Common policy expression and exchange format based on XACML
- GAAAPI/GAAA_tk profile for multidomain AuthZ and pushing policy
- Integrating with existing Access Control and other tools
  - ✓ GT4 Authorization Framework
  - ✓ EGEE gLite Authorisation Framework
- Binding Policy to WSDL service description
  - ✓ Using WS-Security Framework and OGSA/WSRF
- Adding VO and VOMS functionality - for user and resource attributes management
- AuthN and Identity management

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, 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 Advanced Internet Research Group at the University of Amsterdam.

Additional information

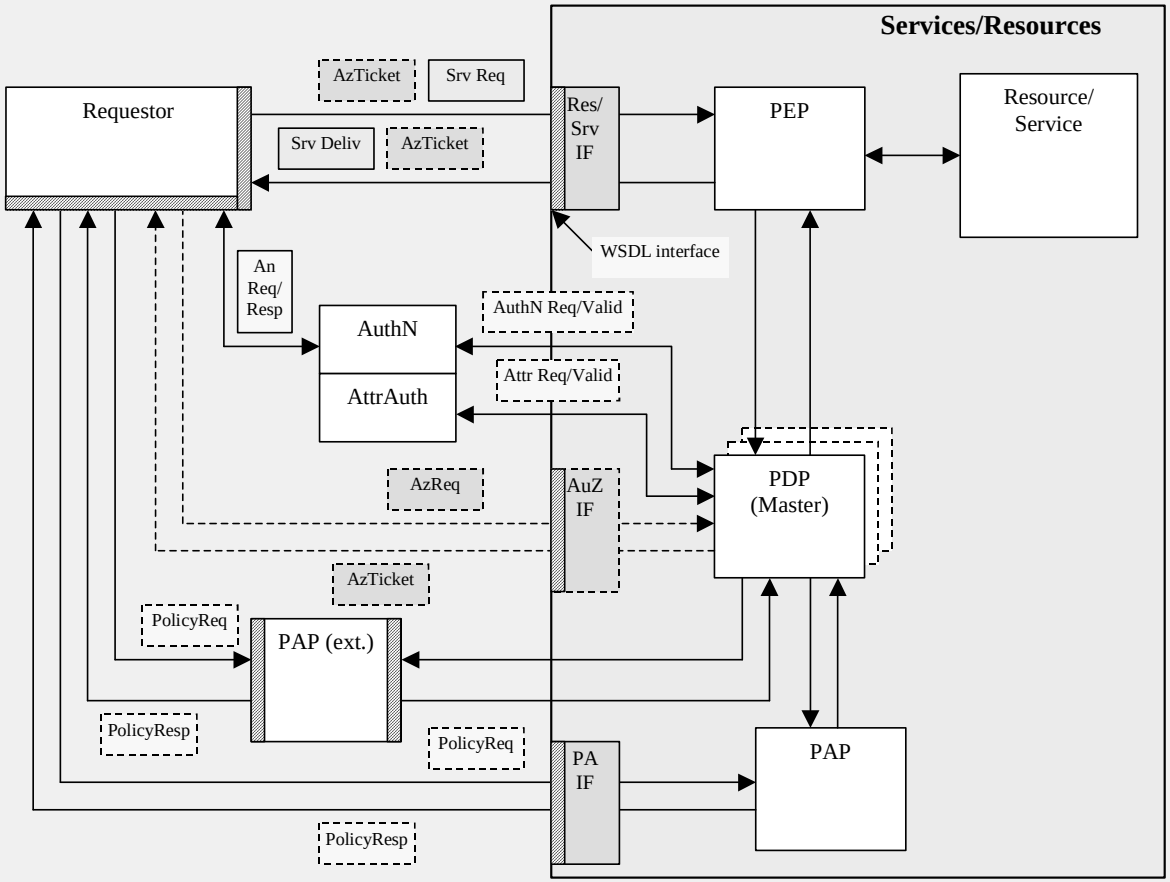
- ✓ Binding Policy to WSDL with WS-PolicyAttachment
- ✓ XACML AuthZ Request and Response messages format and example
- ✓ Detailed AuthZ and AuthN ticket and token examples

Traditional Access Control model – setting up trust and authority relations

- ✓ Policy, attributes semantics and namespaces are known a priory to all participating parties
  - o A requestor knows what information to present to adhere to a specific policy and in what format (although PEP may act as ASM)
- ✓ PEP and PDP locations are known and interacting parties are known
- ✓ Trust relations between PDP, AA and resource are established
  - o 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
  - o Root of policy enforcement hierarchy, like in real life, belongs to the resource owner

- ✓ This approach is not sufficient for effective Service Oriented Architecture (SOA)

Open policy enforcement model in WSA/SOA using WS-PolicyAttachment mechanisms



- 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

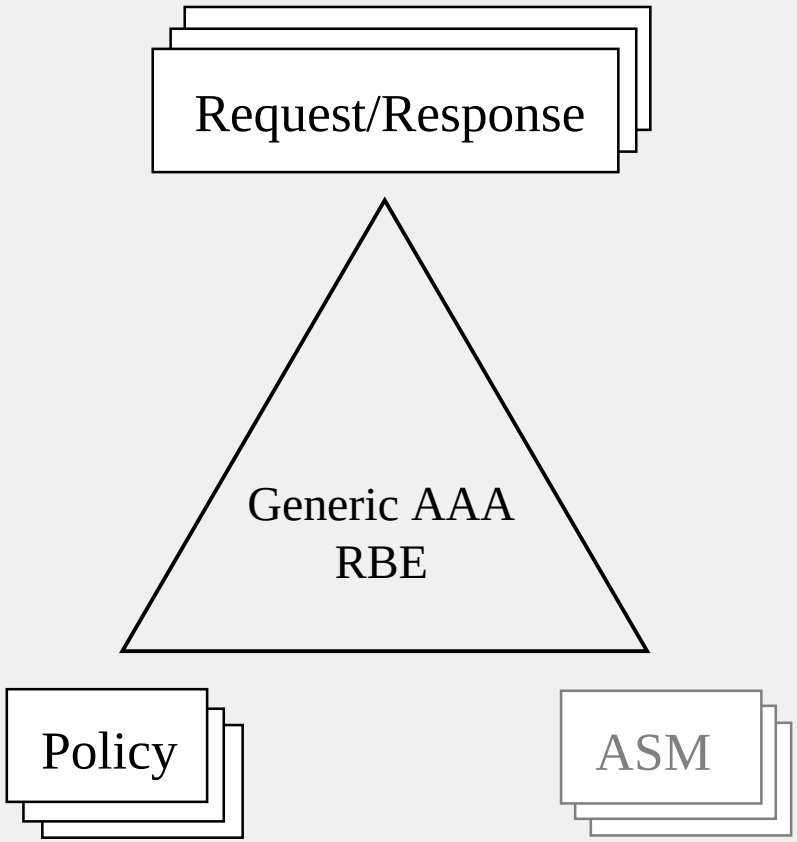
Attaching policy to WSDL - Example

```
<definitions xmlns="http://schemas.xmlsoap.org/wsdl/"
          < …. snip long namespace declaration …. >
    xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy"
    xmlns:cnl="http://cnl.telin.nl/cnl" xmlns:policy="cnl-policy-schema.xsd"
    targetNamespace="http://cnl.telin.nl/cnl">
     <message name="ViewExperimentRequest" wsp:PolicyURIs="cnl-policy-
    02example.xml">
          <part name="coordinateX" type="xs:string"/>
         <part name="coordinateY" type="xs:string"/>
         <part name="zoom" type="xs:int"/>
     </message>

    <<< snip >>>>
     <wsp:PolicyAttachment ... >
          <wsp:AppliesTo>
               <x:DomainExpression/> +
          </wsp:AppliesTo>
          ( <wsp:Policy>...</wsp:Policy> |
          <wsp:PolicyReference>...</wsp:PolicyReference> ) +
          <wsse:Security>...</wsse:Security> ?
          ...
     </wsp:PolicyAttachment>

     <wsp:UsingPolicy wsdl:Required="true"/>
    </definitions>
```

(1) Generic AAA Architecture by AIRG (UvA)

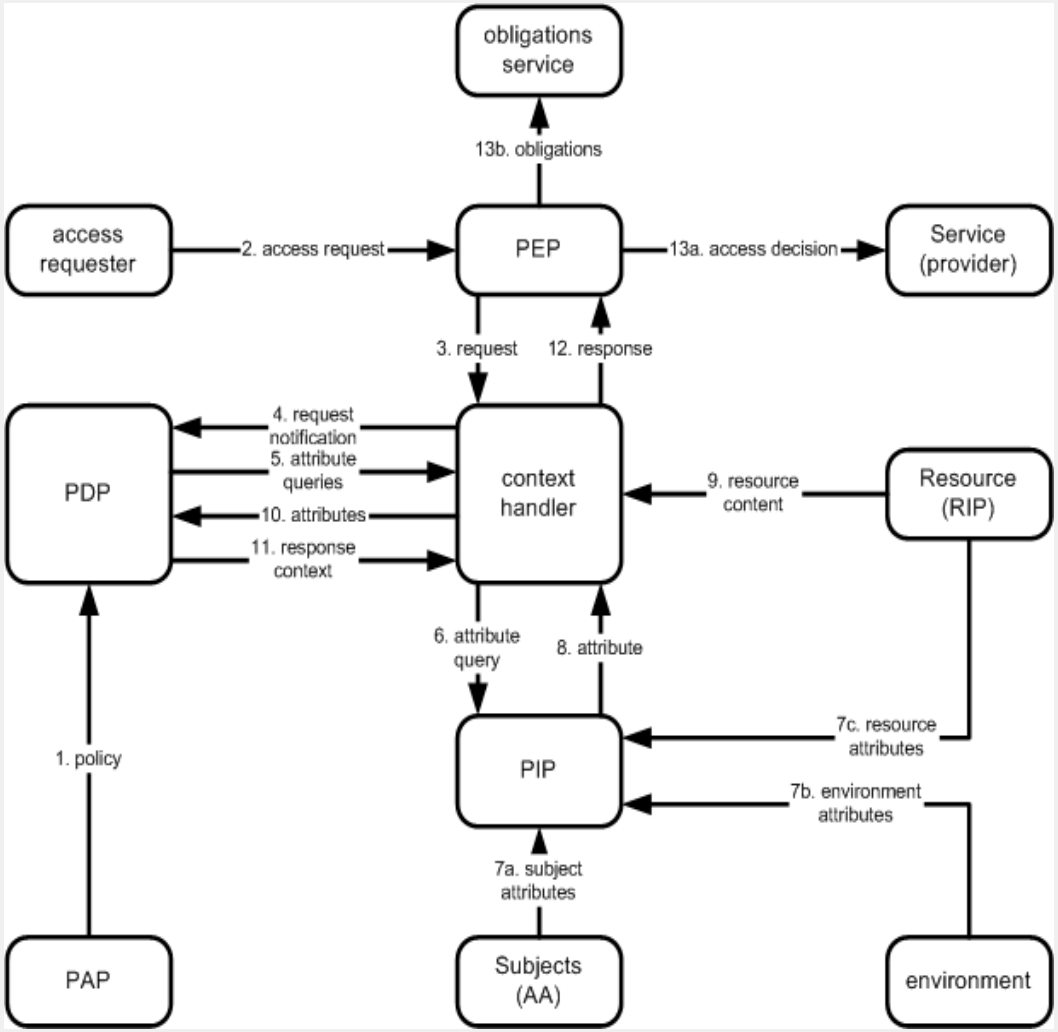


- Policy based Authorization decision
  - ✓ Req {AuthNtoken, Attr/Roles, PolicyTypeId, ConditionExt}
  - ✓ RBE (Req + Policy) => => Decision {ResponseAAA, ActionExt}
  - ✓ ActionExt = {ReqAAAExt, ASMcontrol}
  - ✓ ResponseAAA = {AckAAA/RejectAAA, ReqAttr, ReqAuthN, BindAAA (Resource, Id/Attr)}

•Defined by Resource owner

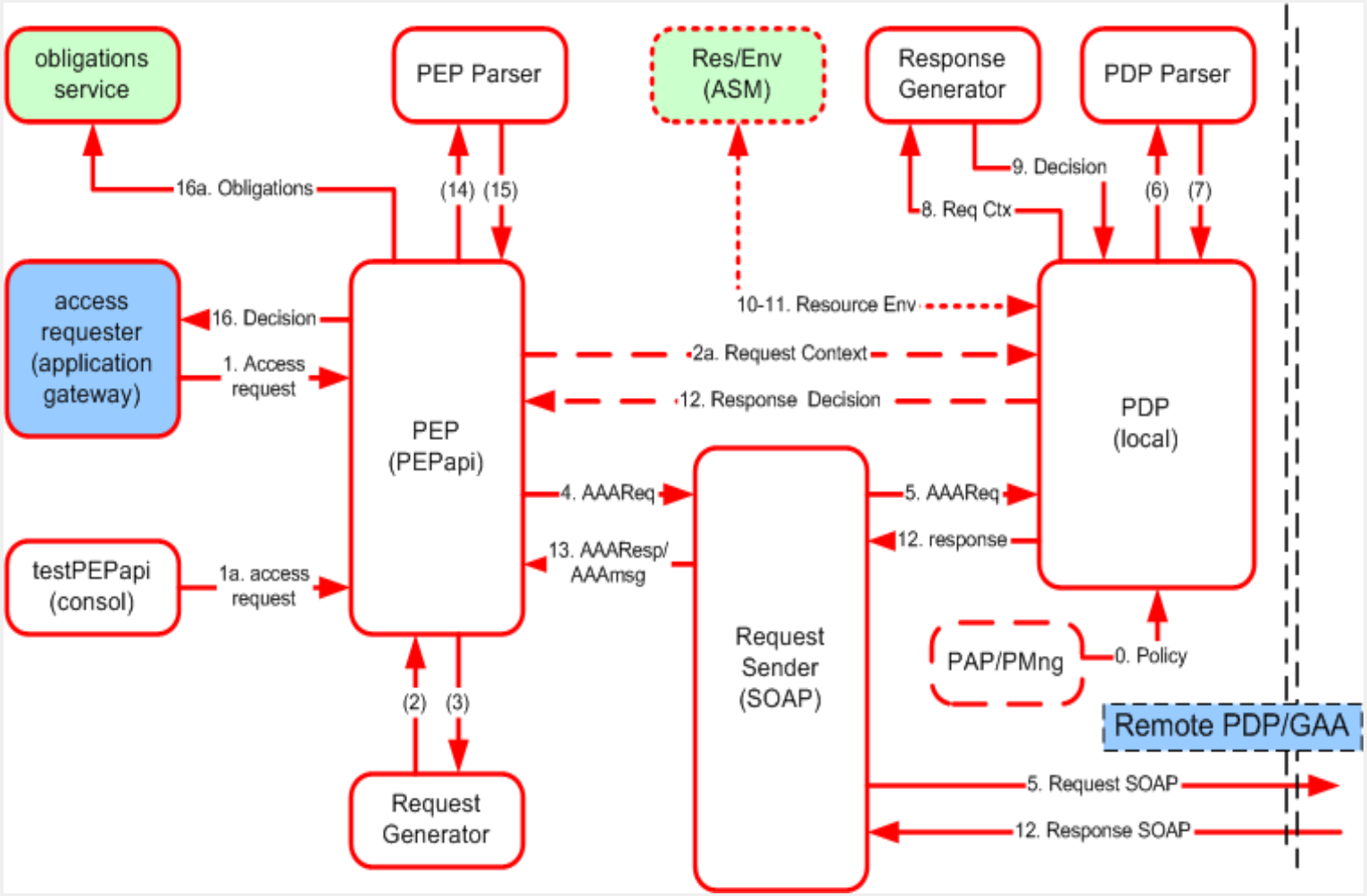
•Translate LogDecision => Action
•Translate State => LogCondition

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

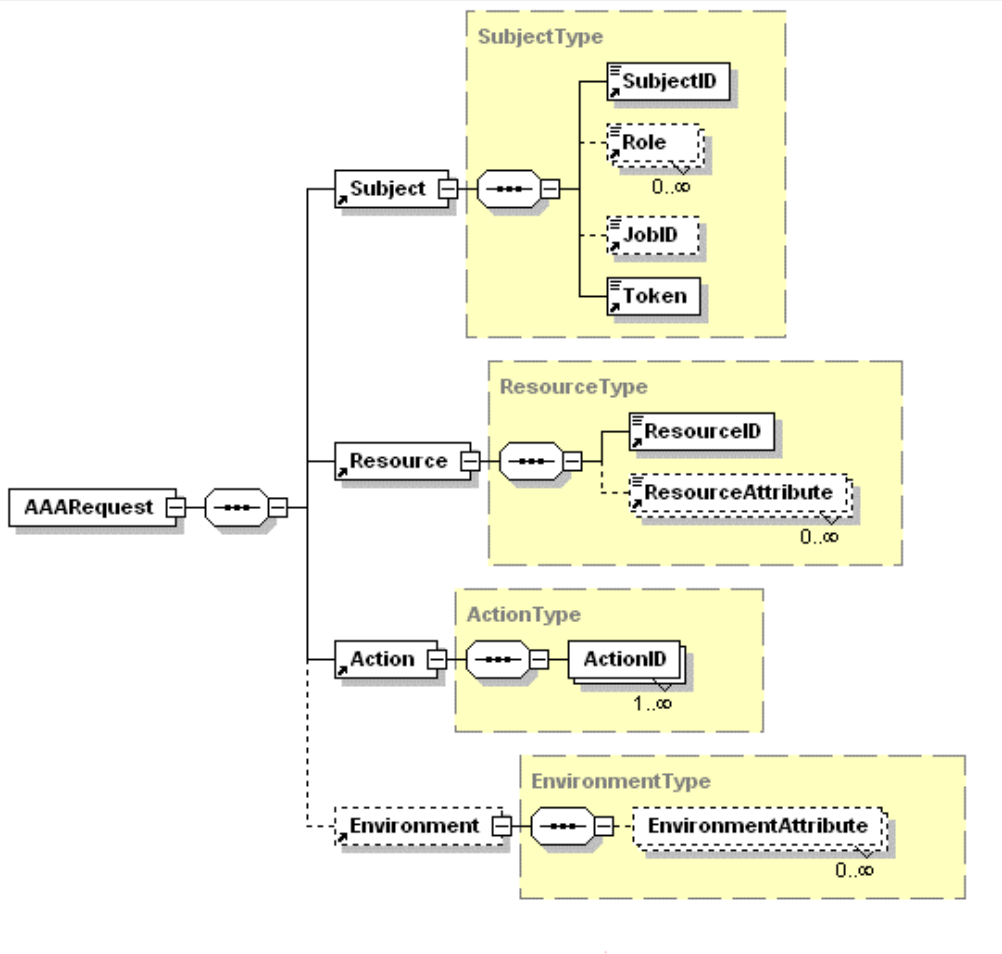


- PEP/AEF - Policy Enforcement Point (authorisation enforcement function)
- PDP/ADF - Policy Decision Point (authorisation decision function)
- PIP - Policy Information Point
- AA - Attribute Authority
- PAP - Policy Authority Point

GAAAPI dataflow diagram (implements RBAC)



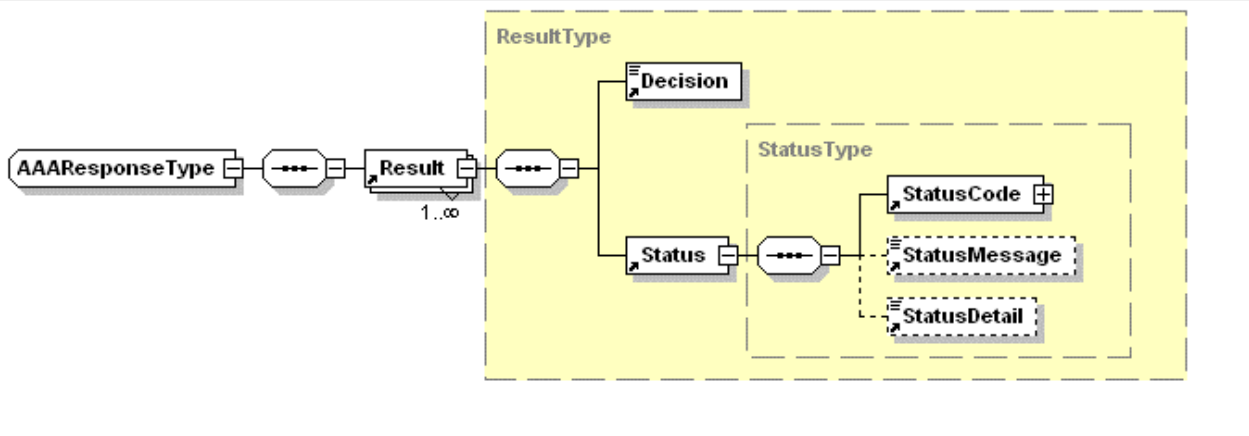
GAAAPI implementation – XACML Request message format




```
<?xml version="1.0" encoding="UTF-8"?>
<AAA:AAARequest
     xmlns:AAA="http://www.AAA.org/ns/AAA
     _BoD"
     xsi:schemaLocation="http://www.AAA.o
     rg/ns/AAA_BoD
     http://146.50.22.64/CNLdemo1.xsd"
     version="0.1" type="CNLdemo1">
  <Subject>
    <SubjectID>
     WHO740@users.collaboratory.nl</Subje
     ctID>
    <Token>
     2SeDFGVHYTY83ZXxEdsweOP8Iok)yGHxVfHo
     m90 </Token>
   <JobID>JobID-XPS1-212</JobID>
   <Role>Analyst@JobID</Role>
  </Subject>
  <Resource>
    <ResourceID>
     http://resources.collaboratory.nl/Ph
     illips_XPS1
     </ResourceID>
  </Resource>
  <Action>

    <ActionID>ControlInstrument</Attribu
     teID>
  </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="ed9d969e1262ba1d3a7f33dbd670dd94">
<cnl:TokenValue>
0IZt9WsJT6an+tIxhhTPtiztDpZ+iynx7K7X2Cxd2iBwCUTQ0n61Szv81DKllWsq75IsHf
   usnm56
zT3fhKU1zEUsob7p6oMLM7hb42+vjfvNeJu2roknhIDzruMrr6hMDsIfaotURepu7QCT0s
   ADm9If
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>
```