Topology related attributes used for Provisioning and Access Control Policy Definition in Multidomain Network Resource Provisioning

Yuri Demchenko
SNE Group, University of Amsterdam

NML-WG meeting, OGF27
13 October 2009, Banff, Canada

Outline

- Network Resource Provisioning model and policy definition use cases
- XACML Policy datamodel
- XACML-NRP attributes – Subject, Resource, Action, Environment
  - Example topology aware policy defintion
- XACML-NRP implementation
  - Resource ID expression format
  - Policy resolution and finding
  - Attributes set/metadata extensibility
- Discussion and suggested security policy related NML attributes

This work was done as a part of the Phosphorus project “Lambda User Controlled Infrastructure for European Research” (October 2006 - June 2009)
http://www.ist-phosphorus.eu/

Network Resource Provisioning (NRP) Model

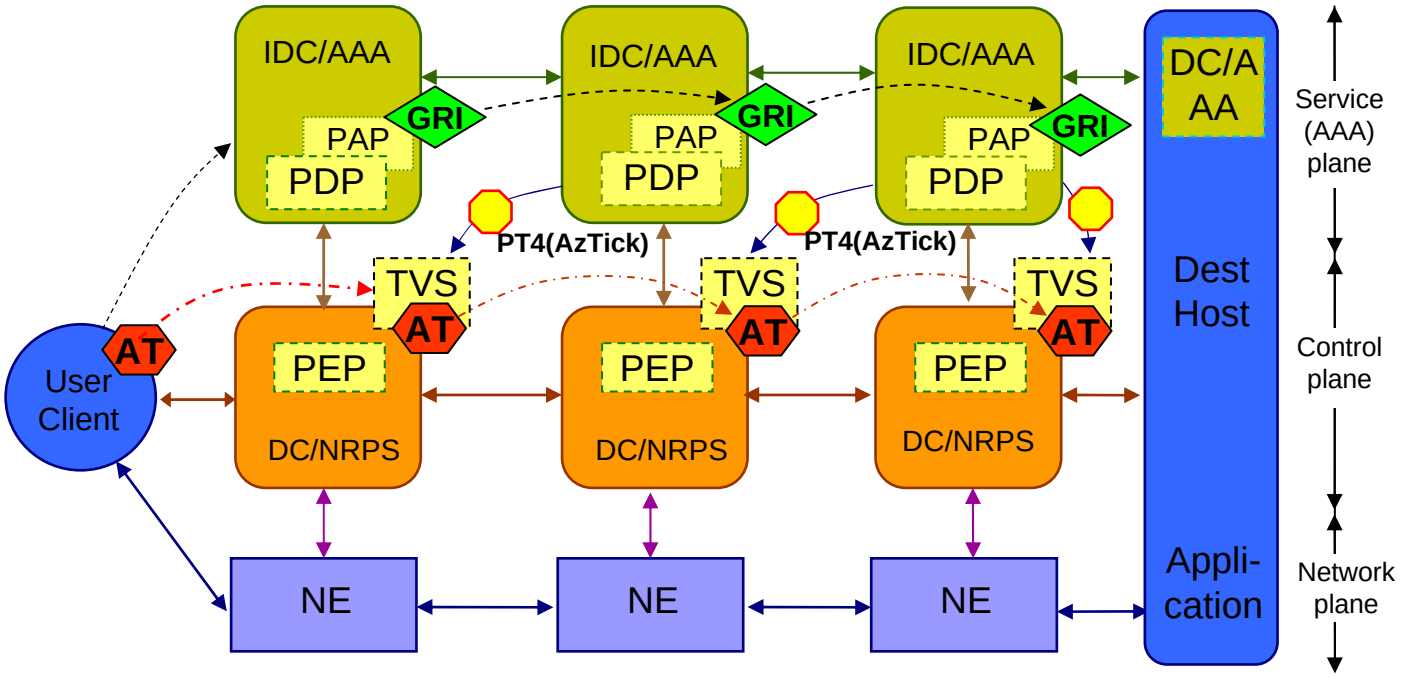
4 major stages/phases in NRP operation/workflow

- (Advance) reservation consisting of 3 basic steps
  - Resource Lookup
  - Resource composition (including options)
  - Component resources commitment, including AuthZ/policy decision, and assigning a global reservation ID (GRI)
- Deployment – reservation confirmation and distributing components/domain configuration (including trusted keys distribution)
- Access (to the reserved resource) or consumption
  - Authorisation session management with AuthZ tickets and tokens
- Decommissioning
  - Provisioning session termination
  - Accounting
- *Relocation (under consideration)*

Rationale

- *Supports the whole provisioned resource life-cycle*
- Specifically oriented on combined Grid-Network resource provisioning
- Integrating resource provisioning into the upper layer scientific workflow

Multidomain Network Resource Provisioning (NRP) – Stages and interdomain communication



IDC/DC – Interdomain/Domain Controller
NRPS – Network Resource Provisioning System
NE - Network Element
AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service

Token based signalling and access control

GRI – Global Reservation ID

AT – Access Token

PT – Pilot Token

AzTicket – AuthZ ticket for multidomain context mngnt

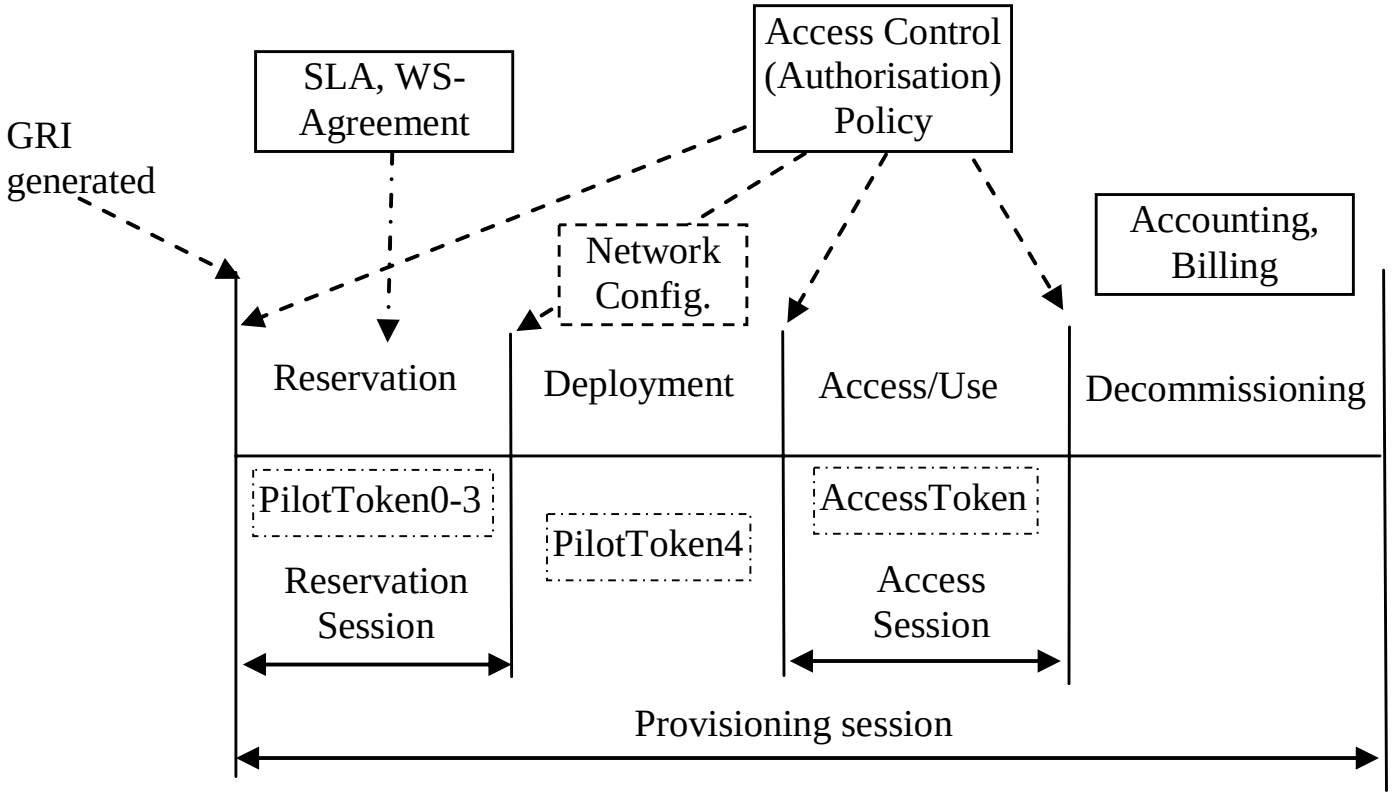
Pilot Token type 1-3 is used at the ***Stage 1 Reservation*** for signalling and interdomain context communication

* As container for GRI and AzTicket

Pilot Token type 4 is used at the ***Stage 2 Deployment*** for setup information communication

Access Token/Ticket is used at the ***Stage 3 Access***

NRP stages and Authorisation session types

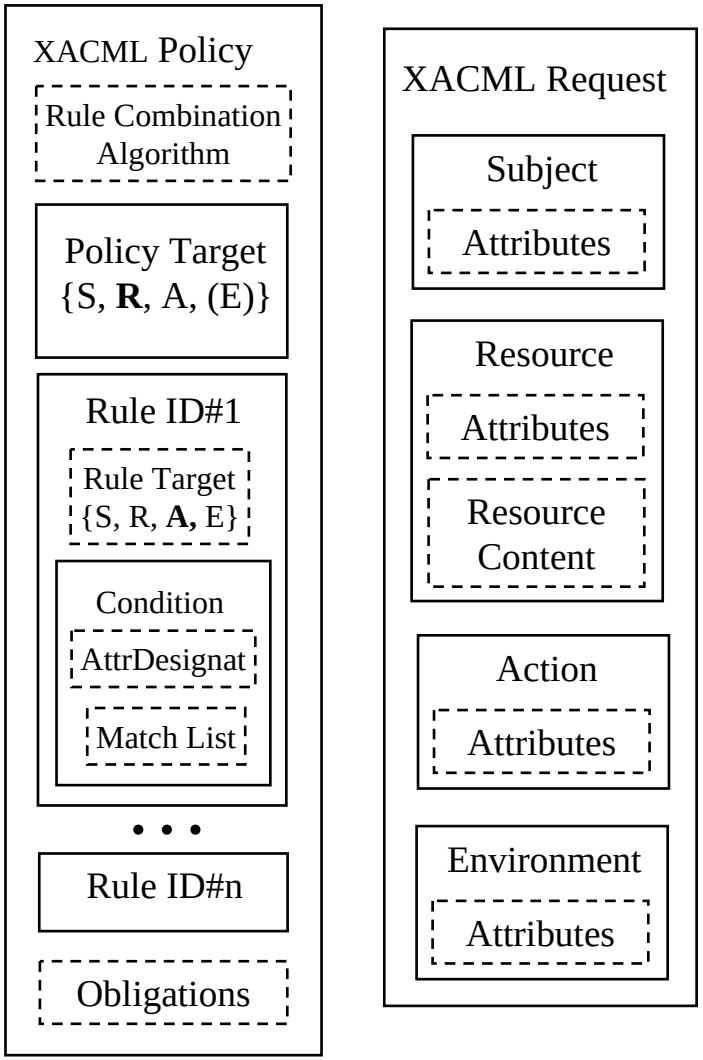


Requires consistent security and session context management

Global Reservation ID (GRI) is created at the beginning of the provisioning session (Reservation stage) and binds all sessions

XACML Policy format and Policy Obligations

- XACML standard specifies XACML policy format and XACML request/response messages
- Policy consists of Policy Target and Rules
  - Policy Target is defined for the tuple Subject-Resource-Action (-Environment)
    - Note: Match function is limited to 2 variables
  - Policy Rule consists of Conditions and may contain Obligations
  - *Policy Obligation defines actions to be taken by PEP on Policy decision by PDP*
- XACML PDP returns all Obligations that match policy decision (defined by attribute “FulfillOn”) from both PolicySet and comprising individual policies
- XACML Request message contains attributes of Subject, Resource, Action, Environment
  - Resource element can contain resource description
  - Environment element may contain additional information, e.g. session related context



XACML-NRP Profile

XACML-NRP Authorisation Interoperability profile for Network Resource Provisioning

- Part of the Phosphorus Project deliverable D.4.3.1 - "GAAA toolkit pluggable components and XACML policy profile for ONRP“ http://www.ist-phosphorus.eu/files/deliverables/Phosphorus-deliverable-D4.3.1.pdf
- Incorporates and extends XACML-Grid profile https://edms.cern.ch/document/929867/1
  - Developed as EGEE-OSG-Globus cooperation and implemented in the Globus and gLite middleware
- Attribute identifiers and attribute identification
  - URL-style and registered namespace http://authz-interop.org/nrp/xacml
    - Both XACML-Grid and XACML-NRP
  - SAML/XACML style – Attribute identifiers are attributes to more generic attribute names

Basic use cases for policy definition in NRP

Access stage

- Use case 1: "User A is only allowed to use user endpoints X, Y and Z"
  - Defined as TNA (Transport Network Address)
- Use case 2: "User A is only allowed to use endpoints in domain N and M“
- Use case 3: “User/Group A is only allowed to invoke method/action X, Y, and Z”
- Use case 4: “User/Group A is only allowed to invoke method X,Y, and Z based on session delegation”
  - Including interdomain access and delegation

Reservation stage

- Use case 5: “Apply {topology restrictions} to the path reservation in the next domain”
- Use case 6: “Check/match {topology/path restrictions} from the previous domain”

Topology description formats/languages

- Topology related attributes enable topology aware policy definition (e.g. use cases 5 and 6)
- 3 topology description formats reviewed
  - Phosphorus Harmony/NSP (XML based)
  - NDL by UvA (RDF based)
  - OSCARS (2008) (XML based)

Example (1) - Harmony Topology description

```
<ns4:Domains>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">dummy</ns3:DomainId>
    <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
    <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">1171</ns3:SequenceNumber>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">
          Virtual dummy domain</ns3:Description>
  <ns3:ReservationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyReservation/services/MyService</ns3:ReservationEPR>
  <ns3:TopologyEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyTopology/services/MyService</ns3:TopologyEPR>
  <ns3:NotificationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyNotification/services/MyService</ns3:NotificationEPR>
  <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">128.0.0.0/16</ns3:TNAPrefix>
  <ns3:avgDelay xmlns:ns3="http://ist_phosphorus.eu/nsp">50</ns3:avgDelay>
  <ns3:maxBW xmlns:ns3="http://ist_phosphorus.eu/nsp">1111</ns3:maxBW>
</ns4:Domains>

RequestContextPath="./xacml-context:Resource/xacml-context:Attribute/xacml-
    context:AttributetValue/ns4:Domains/ns3:avgDelay"
```

Example (2) – NDL (2008) topology description

```
<!-- TDM3.amsterdam1.netherlight.net -->
<ndl:Device rdf:about="#tdm3.amsterdam1.netherlight.net">
      <ndl:name>tdm3.amsterdam1.netherlight.net</ndl:name>
      <ndl:locatedAt rdf:resource="#amsterdam1.netherlight.net"/>
      <ndl:hasInterface rdf:resource="#tdm3.amsterdam1.netherlight.net:501/1"/>
      <ndl:hasInterface rdf:resource="#tdm3.amsterdam1.netherlight.net:501/2"/>
      <ndl:hasInterface rdf:resource="#tdm3.amsterdam1.netherlight.net:505/3"/>
      <ndl:hasInterface rdf:resource="#tdm3.amsterdam1.netherlight.net:505/4"/>
</ndl:Device>
<!-- all the interfaces of TDM3.amsterdam1.netherlight.net -->
<ndl:Interface rdf:about="#tdm3.amsterdam1.netherlight.net:501/1">
      <ndl:name>tdm3.amsterdam1.netherlight.net:POS501/1</ndl:name>
      <ndl:connectedTo rdf:resource="#tdm4.amsterdam1.netherlight.net:5/1"/>
      <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
 </ndl:Interface>
<ndl:Interface rdf:about="#tdm3.amsterdam1.netherlight.net:501/2">
      <ndl:name>tdm3.amsterdam1.netherlight.net:POS501/2</ndl:name>
      <ndl:connectedTo rdf:resource="#tdm1.amsterdam1.netherlight.net:12/1"/>
      <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
 </ndl:Interface>
```

Example (3) – OSCARS (2008) topology description

```
<!-- blue-es1 to blue-es2 -->
<staticPathEntry id="blue-es1-blue-es2">
  <srcEndpoint>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2</srcEndpoint>
  <destEndpoint>urn:ogf:network:domain=blue.pod.lan:node=vlsr3:port=3:link=11.2.5.1</destEndpoint>
  <path id="blue-es1-blue-es2">
     <hop id="1">
       <linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2</linkIdRef>
     </hop>
     <hop id="2">
        <linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=5:link=11.2.3.1</linkIdRef>
     </hop>
     <hop id="3">
        <linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr3:port=5:link=11.2.3.2</linkIdRef>
     </hop>
     <hop id="4">
        <linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr3:port=3:link=11.2.5.1</linkIdRef>
     </hop>
  </path>
  <availableVtags></availableVtags>  <!-- deprecated: leave blank -->
</staticPathEntry>
```

Resource/topology related attributes

Attribute name	Attribute ID	Full XACML attributeId semantics (ns-prefix = http://authz-interop.org/nrp/xacml)
Domain	domain-id	{ns-prefix} /resource/domain-id
Subdomain	subdomain	{ns-prefix} /resource/sub-domain
VLAN	vlan	{ns-prefix} /resource/vlan
TNA	tna (+ tna-prefix)	{ns-prefix} /resource/tna-prefix/tna
Node	node	{ns-prefix} /resource/node
Network path	path	{ns-prefix} /resource/path
Link	link-id	{ns-prefix} /resource/link-id
avrDelay	delay	{ns-prefix} /resource/delay
maxBW	bandwidth-max	{ns-prefix} /resource/bandwidth
Realm	realm	{ns-prefix} /resource/realm {ns-prefix} /realm
Resource type	resource-type	{ns-prefix} /resource/resource-type ({ns-prefix} /resource/device)
Resource federation	federation	{ns-prefix} /resource/federation

- Domain ID (network domain)
- Subdomain
- Node or TNA and TNA prefix
- Interface ID or Link ID
- Device or resource-type
- Link parameters: average delay and maximum bandwidth
- ReservationEPR that may directly or indirectly define the resource federation or security/ administrative domain
- Federation that defines a number of domains or nodes sharing common policy and attributes
- Realm defines project/task related association and may have own namespace

Subject related attributes

Attribute name	**Attribute ID**	**Full XACML attributeId semantics (ns-prefix = http://authz-interop.org/nrp/xacml)**
Subject ID	subject-id	{ns-prefix} /subject/subject-id
Subject confirmation *)	subject-confdata	{ns-prefix} /subject/subject-confdata
Subject context **)	**subject-context**	**{ns-prefix} /subject/subject-context**
Subject group	subject-group	{ns-prefix} /subject/subject-group
Subject role	subject-role	{ns-prefix} /subject/subject-role
Subject federation	Federation	{ns-prefix} /subject/federation

*) Subject confirmation attribute may contain subject credentials

- Currently supported SAML2.0, Proxy/VOMS Attribute Certificate, Unicore6 SAML2, AuthN Ticket
- Validated by PEP before sending to PDP

**) Subject context is used for policy resolution

Action related attributes and enumerated values

Attribute name	**Attribute ID**	**Full XACML attributeId semantics (ns-prefix = http://authz-interop.org/nrp/xacml)**
Action ID	action-id	{ns-prefix} /action/action-id
Action type	action-type	{ns-prefix} /action/action-type/{value}

Attribute name	**Enumerated value**	**XACML attribute value (ns-prefix = http://authz-interop.org/nrp/xacml)**
Action type	create-path	{ns-prefix} /action/action-type/create-path
	activate-path	{ns-prefix} /action/action-type/activate-path
	cancel	{ns-prefix} /action/action-type/cancel
	access	{ns-prefix} /action/action-type/access

Environment related attributes

Environment attributes define additional required for the policy decision

- Previous domain confirmation in multidomain NRP
- Authorisation context
  - AuthZ session credentials or AuthZ ticket/token
- Obligations, Delegation (or account mapping) from the previous domain
  - User ID or group to which access is delegated
  - Actions which need to be taken when processing request or granting access
  - Topology restrictions, e.g. minimal bandwidth, delay, VLAN, etc.

XACML-NRP Policy Obligations

Suggested policy obligations for multidomain NRP

- Intra-domain network/VLAN mapping for cross-domain connections
  - Can be used to map external/interdomain border links/endpoints to internal VLAN and sub-network
- Account mapping (inter/cross-domain)
- Type of service (or QoS) assigned to a specific request or policy decision
- Quota assignment
- Service combination with implied conditions (e.g., computing and storage resources)
- Usable resources e.g. number of access/view, volume of traffic, etc
  - *Advance Resource Reservation (ARR) type – Fixed, Deferrable, Malleable*

Example(1): Resource and Subject attributes and Policy resolution

PEP API Request components

```
ResourceInputURI =
   "http://testbed.ist-phosphorus.eu/viola/harmony/source=10.3.1.16/target=10.7.3.13“
ResourceMap = resource-id=http://testbed.ist-phosphorus.eu/viola/harmony,
        resource-realm=testbed.ist-phosphorus.eu
        resource-domain=viola
        resource-type=harmony
        source=10.3.1.16
        target=10.7.3.13
SubjectMap = subject-id=WHO740@users.testbed.ist-phosphorus.eu,
        subject-role=researcher, subject-context=demo041,
        subject-confdata=“IGhA11...8bUktYh”}

Policy file = {policy-dir}/nrp/testbed.ist-phosphorus.eu/viola-policy-harmony-
   demo041.xml
```

Resolution functionality is supported by GAAA-TK/API library functional components:
NamespaceResolver, AttributeResolver, PolicyResolver

Example (2): XACML Request message

```
<Request>
<Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="http://testbed.ist-
    phosphorus.eu/phosphorus/aaa/AttributeIssuer" IssueInstant="2008-12-03T12:10:21.218000000+01:00">
    <AttributeValue>WHO740@users.testbed.ist-phosphorus.eu</AttributeValue></Attribute>
<Attribute AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-role">
    <AttributeValue>researcher</AttributeValue></Attribute>
<Attribute AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-context">
    <AttributeValue>demo041</AttributeValue></Attribute>
<Attribute AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-confdata">
    <AttributeValue>aaa:authn:gaaapi:subject:confirmed</AttributeValue></Attribute>
</Subject>
<Resource>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
    <AttributeValue>http://testbed.ist-phosphorus.eu/viola/harmony</AttributeValue></Attribute>
<Attribute AttributeId="http://authz-interop.org/AAA/xacml/resource/resource-realm">
    <AttributeValue>testbed.ist-phosphorus.eu</AttributeValue></Attribute>
<Attribute AttributeId="http://authz-interop.org/AAA/xacml/resource/resource-domain">
    <AttributeValue>viola</AttributeValue></Attribute>
<Attribute AttributeId="http://authz-interop.org/AAA/xacml/resource/target">
    <AttributeValue>10.7.3.13</AttributeValue></Attribute>
<Attribute AttributeId="http://authz-interop.org/AAA/xacml/resource/source">
    <AttributeValue>10.3.1.16</AttributeValue></Attribute>
</Resource>
<Action>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" >
    <AttributeValue>create-path</AttributeValue></Attribute>
</Action></Request>
```

Example (3) – Topology/Path information in ResourceContent

```
<xacml-context:Resource><xacml-context:ResourceContent>
<ns4:Domains>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">dummy</ns3:DomainId>
    <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
    <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">1171</ns3:SequenceNumber>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">
          Virtual dummy domain</ns3:Description>
  <ns3:ReservationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyReservation/services/MyService</ns3:ReservationEPR>
  <ns3:TopologyEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyTopology/services/MyService</ns3:TopologyEPR>
  <ns3:NotificationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">
          http://localhost:8080/nrpsDummyNotification/services/MyService</ns3:NotificationEPR>
  <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">128.0.0.0/16</ns3:TNAPrefix>
  <ns3:avgDelay xmlns:ns3="http://ist_phosphorus.eu/nsp">50</ns3:avgDelay>
  <ns3:maxBW xmlns:ns3="http://ist_phosphorus.eu/nsp">1111</ns3:maxBW>
 </ns4:Domains>
</xacml-context:ResourceContent></xacml-context:Resource>
```

xacml:RequestContextPath="./xacml-context:Resource/xacml-context:ResourceContent/ xacml-context:Attribute/xacml-context:AttributetValue/ns4:Domains/ns3:avgDelay"

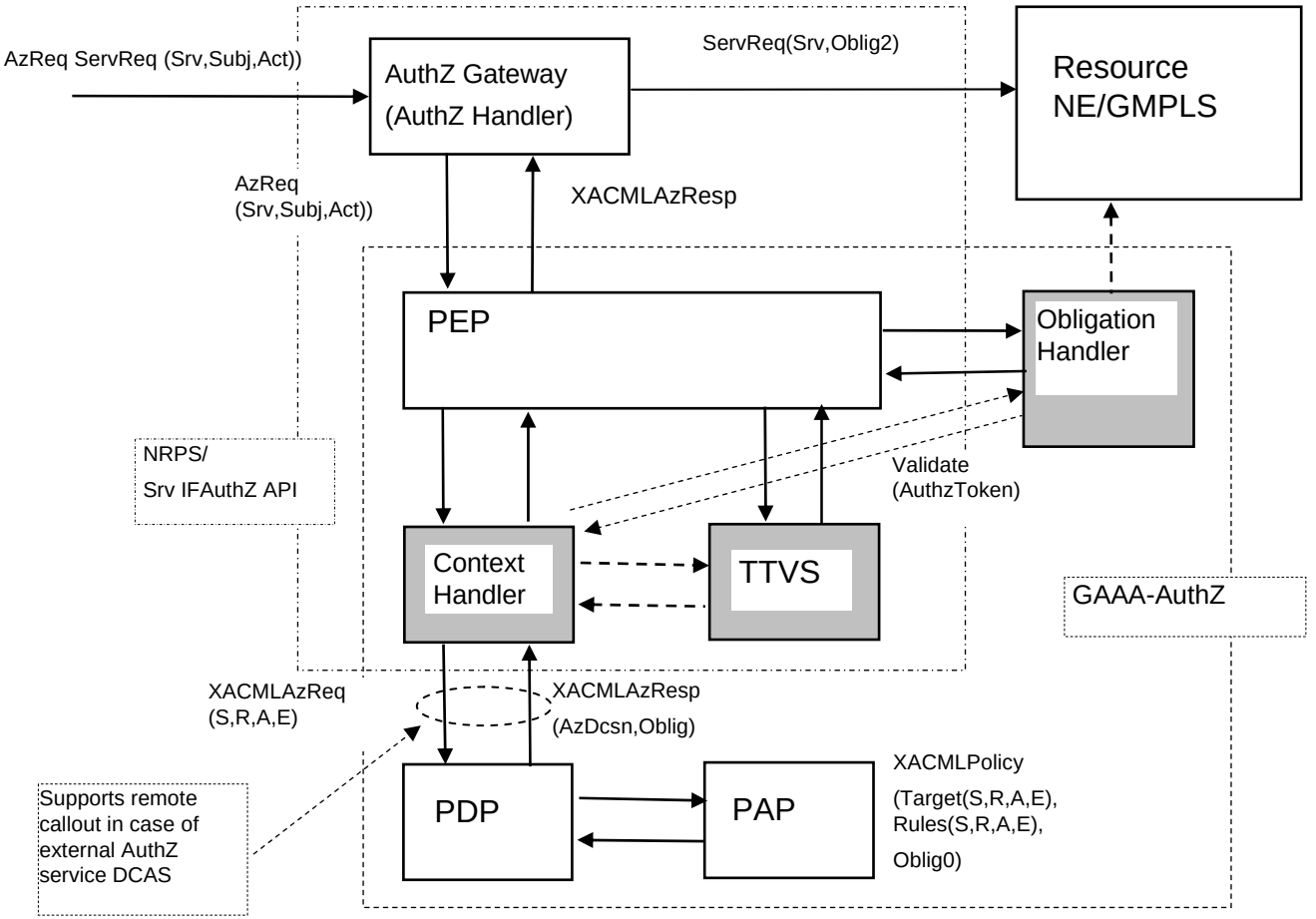
Example (3) - XACML Policy Rule to match ResourceContent

```
<Rule RuleId="urn:oasis:names:tc:xacml:2.0:scas-policy:example001:rule" Effect="Permit">
    <Target/>
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-greater-than">
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">100</AttributeValue>
     </Apply>
     <AttributeSelector RequestContextPath="RequestContextPath=
           "./xacml-context:Resource/xacml-context:Attribute/xacml-context:AttributetValue/
                    ns4:Domains/ns3:avgDelay"
          MustBePresent="true" DataType="http://www.w3.org/2001/XMLSchema#integer"/>
    </Condition>
</Rule>
```

XACML-NRP implementation – GAAA-TK Java library

- XACML-NRP profile is implemented in the GAAA-TK Java library
  - *As configurable metadata/constants set (XML metadata file and Java constants)*
  - Supports also XACML-Grid profile
- GAAA-TK library provides all necessary AuthZ mechanisms and service components to support AuthZ sessions context and Obligations handling
  - AuthZ ticket format for extended interdomain AuthZ session management
  - Supports Pilot token based Interdomain signalling and access control with Access tokens
  - Can be used and ensure signalling and access control transparency at all Networking layers (Service, Control and Data planes)
- Integrated into the Phosphorus project Network Service Plane (NSP Harmony) test-bed and uses simple XACML policy model
- Recent Version 0.8 is available from
  http://staff.science.uva.nl/~demch/projects/aaauthreach/index.html

GAAA Toolkit pluggable AAA/AuthZ components



The proposed model intends to comply with both the generic AAA-AuthZ framework and XACML AuthZ model

- ContextHandler functionality can be extended to support all communications between PEP-PDP and with other modules
- Obligation Handler supports OHRM
- TTVS supports session based credentials – Access and Pilot tokens and tickets

TTVS – Ticket and token validation and handling service

Future developments

- Adopting XACML-NRP attributes/metadata to actual NML and NSI attributes and AAA interface definition
- Considering moving XACML-Grid and XACML-NRP profiles to the OGF standardisation process
- Developing conformance test for XACML-Grid and XACML-NRP profiles

- Expected future development framework – newly approved EU project GEYSER “Generalised Architecture for Dynamic Infrastructure Services”
  - On-demand network infrastructure provisioning
  - Policy based SLA negotiation and Network Resource Provisioning model

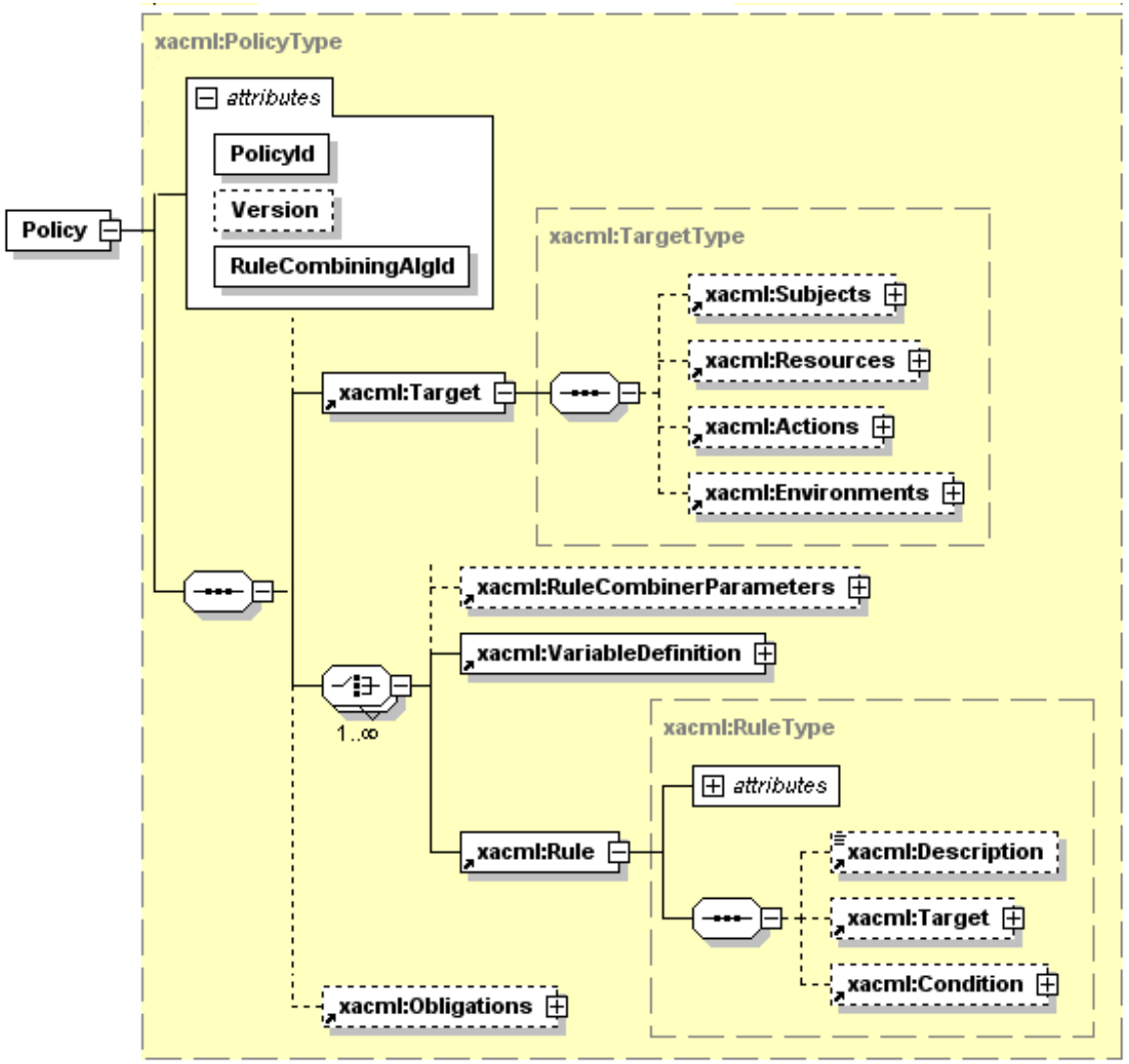
Suggestions for security related NML/topology attributes

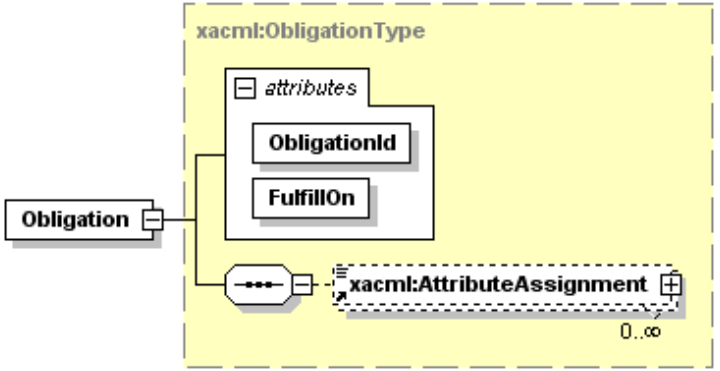
- Path and/or segment definition and description format
- Definition of administrative and security domains
  - In addition to network domain (is it based on DNS domain/subdomain?)
- Metadata configuration file binding instant topology/segment/path description to infrastructure related services
  - Namespace resolution service, AAA services/authorities, Policy RefID/authority, trust anchors
- Is path finding in the scope of NML-WG?
  - It can be conditional and may require policy enforcement
- Need a way/agreement to match network/topology related attributes between NML-WG and NSI-WG
  - Is a Logical (Infrastructure) Composition Layer a solution?

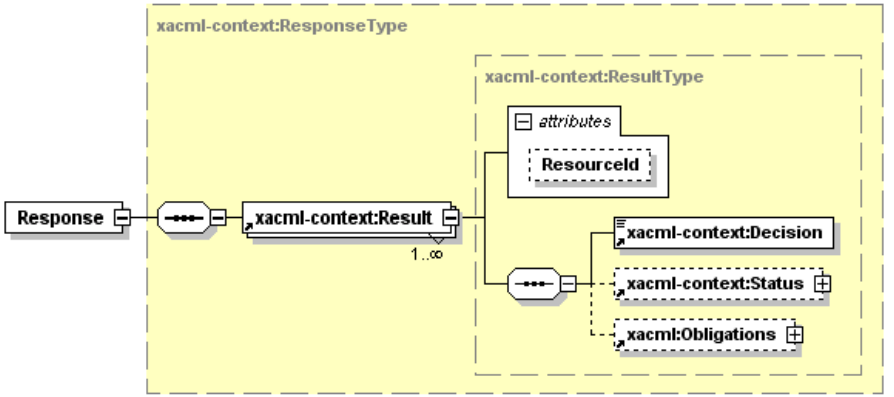
Additional information

- XACML2.0 datamodel and Obligations definition
- Domain definition and domain related security context
- Administrative domain vs Security domain vs Security Association

XACML2.0 Policy Datamodel







XACML Response message contains all Obligations that match policy decision (defined by attribute “FulfillOn”) from both PolicySet and comprising individual policies

XACML Policy Obligations - Definition

Policy Obligation is one of the policy enforcement mechanisms

- ***Obligations*** are a set of operations that must be performed by the ***PEP*** in conjunction with an ***authorization decision*** [XACML2.0]

Obligations semantics is not defined in the XACML policy language but left to bilateral agreement between a PAP and the PEP

PEPs that conform with XACMLv2.0 are required to deny access unless they understand and can discharge all of the <Obligations> elements associated with the applicable policy

Element <Obligations> / <Obligation>

- The <Obligation> element SHALL contain an ***identifier*** (in the form of URI) for the obligation and a set of attributes that form arguments of the action defined by the obligation. The FulfillOn attribute SHALL indicate the effect for which this obligation must be fulfilled by the PEP

Policy definition assumptions for NRP

- Users and resources are described/identified by their unique ID's and may have also assigned attributes, e.g.
  - User attrs: user group, role, federation
  - Resource attrs: domain/subdomain, resource type, level of service
- Users and resources (domains and endpoints) may be organised/associated into administrative and/or security domains or federations
  - A user and a resource can be a member of one or multiple associations
- Different domains and endpoints participating in network connection (for which the authorisation is requested) may belong to different federations or security associations
- Only authenticated user may have access to protected resources
  - User authentication is confirmed by issuing AuthZ assertion by trusted AuthN service or creating user related security context environment of the started process
- User authentication may be resulted in the following:
  - service or process session initiation;
  - release of the user attributes or credentials;
- Depending on the user attributes (federations, groups, roles) the user can be assigned specific level of service
  - To access a network resources a user identity may need to be mapped to a specific (pool) account

Administrative domain vs Security domain vs Security Association

- Domains can be considered as network, administrative or security
  - Network domains are more static
  - Administrative domain is managed by the resource owner (or user administration)
  - Security domain is defined by common trusted identity or attribute management authority
- Security association
  - Security association can be created dynamically, e.g. for managing project, resource provisioning agreement
    - VO or Shibboleth federation are two examples
  - Authorisation session as a kind of security association

Multi-domain NRP – Domain definition and domain related security context

Domains are defined (as associations of entities) by a common policy under single administration, common namespaces and semantics, shared trust,etc.

Domain related security context may include

- namespace aware names and ID's
- policy references/ID's
- trust anchors (CA)
- authorities reference (AAA, AuthZ, AuthN, Policy Authority, CA)
- Additionally, each domain may have/create own dynamic/session related security context (at the reservation and access stages)

Multi-domain NRP AuthZ infrastructure

- Multiple policies processing and combination, including obligated/conditional policy decisions and delegation
- Attributes/rules mapping/converting based on inter domain trust management infrastructure
- Policy support for different logical organisation of resources, including possible constraints on resource combination and interoperation