Attributes used for Authorisation
in
Network Resource Provisioning

(XACML-NRP Authorisation Interoperability Profile for NRP)

Yuri Demchenko

System and Network Engineering Group
University of Amsterdam

NML-WG, OGF 23
2 June 2008, Barcelona

Outline

- AAA/AuthZ Architecture for Optical Network Resource Provisioning (NRP)
  - “Provisioning – Deployment/Activation – Access/Usage”
- Basic use cases for policy definition in NRP
- Technologies for interoperability – SAML and XACML
- Defining Attributes for AuthZ in NRP
  - Network/topology related attributes
  - Subject related attributes
  - Action related attributes
  - Environment related attributes

Background for this research

- EU funded Phosphorus Project “Lambda User Controlled Infrastructure for European Research” (EC Contract number 034115)
- University of Amsterdam SNE Group ongoing research on NRP and GAAA-AuthZ – Generic Authentication, Authorization, Accounting (GAAA) AuthZ Framework
- XACML-NRP profile is based on and considered as extension to XACML-Grid profile by EGEE, OSG, Globus

Draft document – Work in Progress

XACML Authorisation Interoperability profile for Network Resource Provisioning. Phosphorus technical document

- Initial draft - http://staff.science.uva.nl/~demch/projects/aaauthreach/draft-interop-xacml-nrp-profile-00.pdf
- Next release (planned end of June 2008) - http://staff.science.uva.nl/~demch/projects/aaauthreach/draft-interop-xacml-nrp-profile-01.pdf

Related document

“An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids" (Joint project by EGEE, OSG, GT). Version 1.0, May 16, 2008.

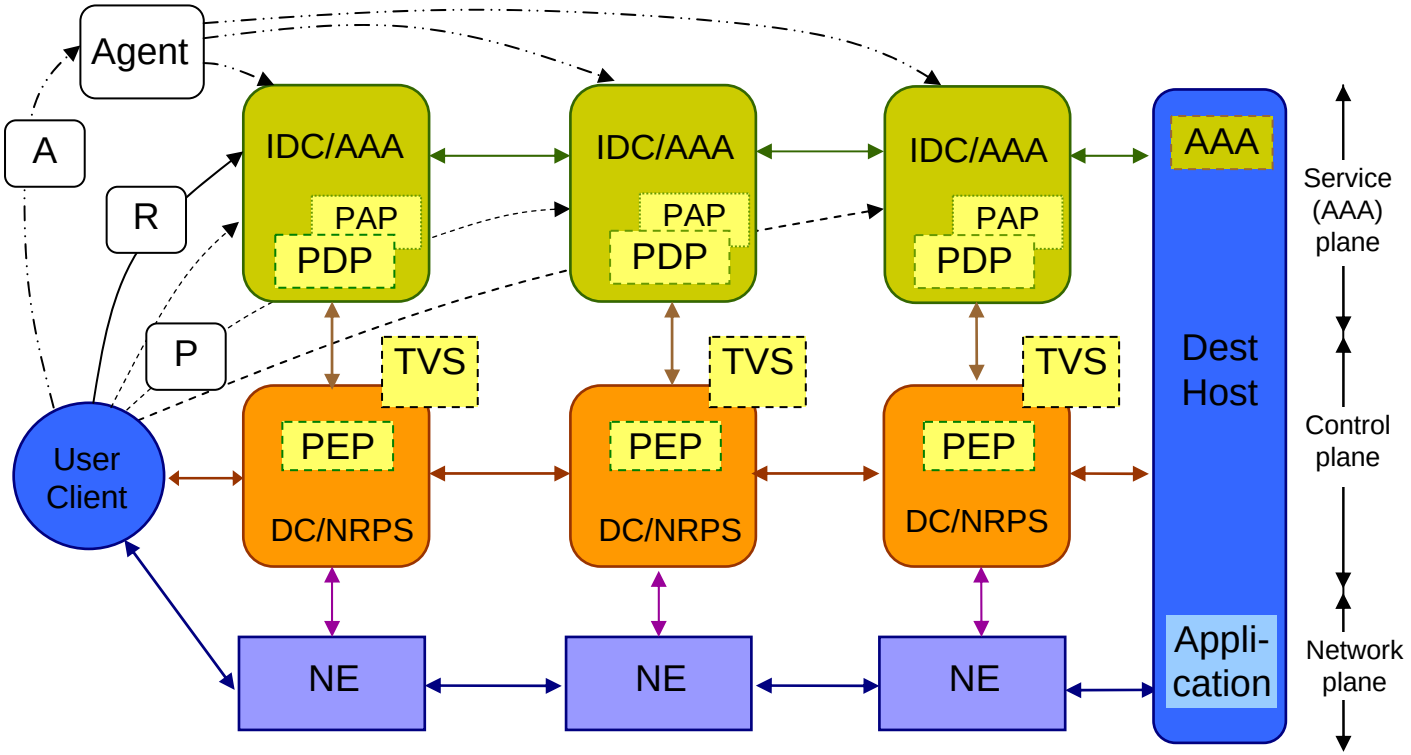
- http://home.fnal.gov/~garzogli/privilege/AuthZInterop/tmp/AuthZInterop XACML Profile v1.0.pdf

Network Resource Provisioning (NRP)

3 stages/phases in NRP/CRP operation

- Reservation consisting of 3 basic steps
  - Resource Lookup
  - Resource composition (including options)
  - (Advance) Network resources reservation, including AuthZ/policy decision, and assigning a global reservation ID (GRI)
- Deployment/Activation
  - Confirmation – additional step that may be required to finalise reservation
- Access (to the reserved resource) or consumption (of the consumable resource)
  - Token or ticket based reservation/AuthZ decision enforcement

Multidomain Network/Complex Resource Provisioning



Provisioning sequences

- Agent (A)
- Polling (P)
- Relay (R)

Token based policy enforcement

GRI – Global Reservation ID

AuthZ tickets for multidomain context mngnt

IDC – Interdomain Controller

DC – Domain Controller

NRPS – Network Resource Provisioning System

AAA – AuthN, AuthZ, Accounting Server
PDP – Policy Decision Point
PEP – Policy Enforcement Point
TVS – Token Validation Service
KGS – Key Generation Service

Basic use cases for policy definition in NRP

Use case 1: "User A is only allowed to use user endpoints X, Y and Z", or

Use case 2: "User A is only allowed to use endpoints in domain N and M"

Policy definition assumptions

- 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

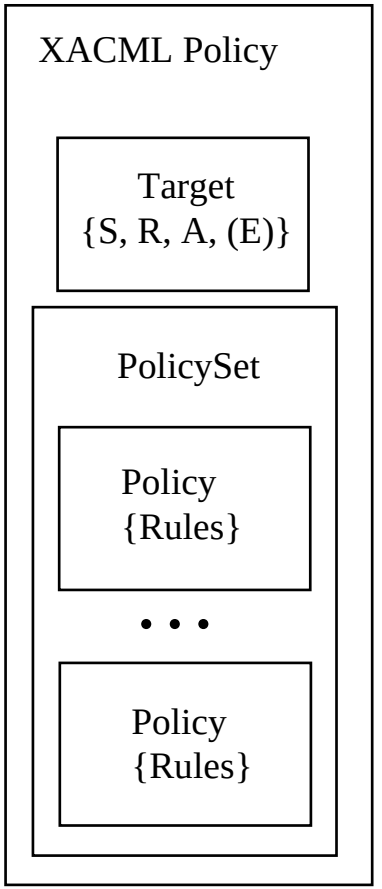
XACML Policy format

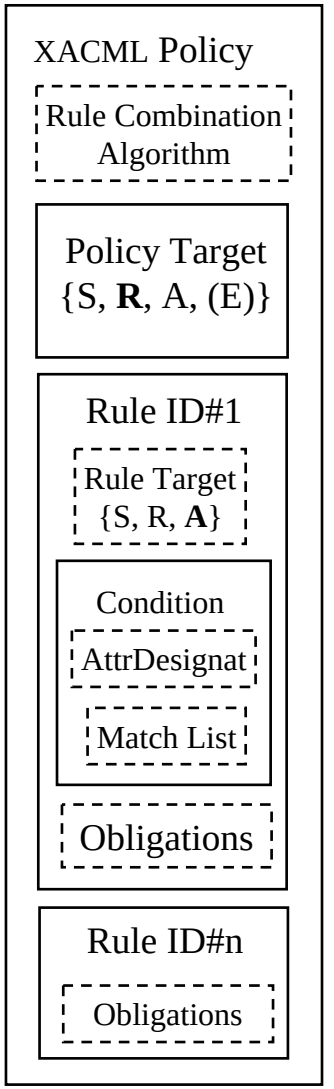
Policy consists of Policy Target and Rules

- Policy Target is defined for the tuple Subject-Resource-Action (-Environment)
- Policy Rule consists of Conditions and may contain Obligations
- Obligation defines actions to be taken by PEP on Policy decision by PDP

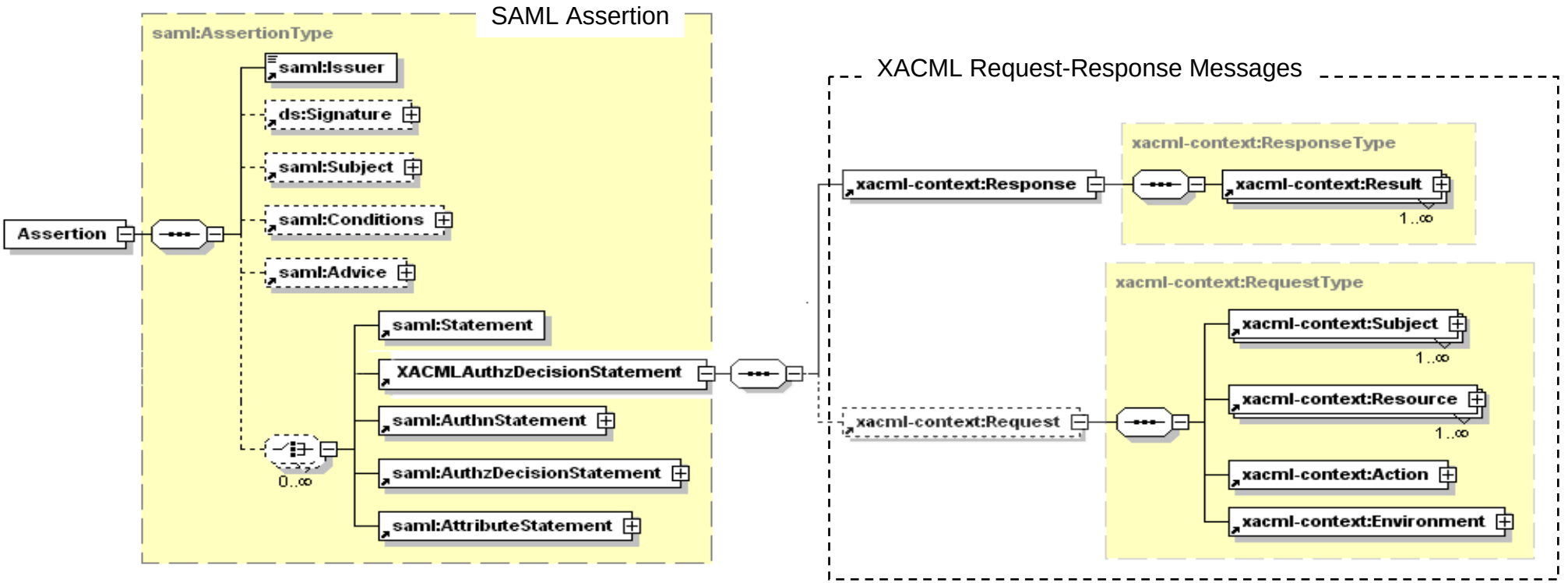
Policy obligation use examples

- Account mapping
- Quota or credit assignment
- Logging, accounting





SAML-XACML Request/Response messages



XACMLRequest (Resource, Subject, Action, Environment)

XACML Request-Response messages are enclosed into the SAML2.0 Assertion or SAML2.0 protocol messages

XACML Request message - Example

```
<xacml-context:Request xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xacml-
    context="urn:oasis:names:tc:xacml:1.0:context" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:context aaa-msg-xacml-01.xsd">
  <xacml-context:Subject Id="subject"    SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-
    subject">
    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" admin@gaaa.virtlab.nl ">
      <xacml-context:AttributeValue>WHO740@users.project.organisation.nl</xacml-context:AttributeValue>
    </xacml-context:Attribute>
    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subjconfdata"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" admin@gaaa.virtlab.nl ">
      <xacml-context:AttributeValue>2SeDFGVHYTY83ZXxEdsweOP8Iok)yGHxVfHom90</xacml-context:AttributeValue>
    </xacml-context:Attribute>
    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" admin@gaaa.virtlab.nl ">
      <xacml-context:AttributeValue>Analyst</xacml-context:AttributeValue>
    </xacml-context:Attribute>
  </xacml-context:Subject>
  <xacml-context:Resource>
    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="admin@gaaa.virtlab.nl">
      <xacml-context:AttributeValue>Resource-ID-here</xacml-context:AttributeValue>
    </xacml-context:Attribute>
  </xacml-context:Resource>
    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="admin@gaaa.collaboratory.nl">
      <xacml-context:AttributeValue>assign-time</xacml-context:AttributeValue>
    </xacml-context:Attribute>
  </xacml-context:Action>
</xacml-context:Request>
```

Resource related Attributes – Topology description formats

- Actually depends on the used/target topology description format
- 3 topology description formats were reviewed
  - Phosphorus NSP/WP1 topology description
  - NDL by UvA
  - OSCARS (currently used)

- Examples AuthZ decision request
  - Is user A allowed to access this reserved path given known (multidomain) network topology?
  - Needs to put some topology attributes into the policy definition

Example of the Resource attributes expression

Attribute name	**Attribute ID**	**Full XACML attributeId semantics (ns-prefix = http://authz-interop.org/nrp/xacml)**
Domain ID	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
Link	link-id	{ns-prefix} /resource/link-id
avrDelay	delay	{ns-prefix} /resource/delay
maxBW	bandwidth-max	{ns-prefix} /resource/bandwidth
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 (or relationship)
- VLAN
- Node or TNA and TNA prefix, or
- Interface ID
- Device or resource-type
- Link ID
- 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

Administrative vs Security domain vs Security Association

- Domains can be considered as administrative and security
  - 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

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

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

- Last-domain conformation
- Authorisation context
  - AuthZ session credentials or AuthZ ticket
- Delegation or Obligations 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

Future developments and Discussion

- Defining XACML-NRP attributes and policy profile
  - Initial draft is available
- Implementing XACML-NRP profile in the GAAA-AuthZ Toolkit
  - Simple XACML policy use cases

- Issues for discussion and liaison with NML-WG
  - Considering different topology description formats
  - Considering different network resource models (e.g., tree, hierarchical)
  - Special attributes for authorisation