

# XACML Authorisation Interoperability profile for Network Resource Provisioning<sup>1</sup>

## Attributes used for authorisation in network resource provisioning

Phosphorus technical document, Draft version 0.1, July 10, 2008

Editor - Yuri Demchenko

Contributors – Yuri Demchenko, (Expected - Fred Wan, Alex Willner, Joan Antoni García Espín)

## Goal and scope of this document

The goal of this document is to provide information about the proposed XACML-NRP attributes profile for general Network Resource Provisioning (NRP) which emerged as a result of developing interoperable multidomain Authorisation infrastructure in the framework of the Phosphorus project and numerous inter-project cooperation links.

This profile is built upon the XACML-Grid attributes profile defined jointly by EGEE, OSG and GT and is suggested to be used as complimentary for Grid-enabled network resources.

The document summarises the recent and on-going discussions in the Phosphorus projects between work packages and with other cooperative activities and developments in the area of creating consistent multidomain AuthZ infrastructure for on-demand optical network resource provisioning. This activity is also considered in relation/connection to the authorisation standardisation activity by the OGSA AUTHZ-WG at the OGF.

The document provides a short overview of the existing formats for network topology description as a basis for defining XACML policy profile and templates and for defining a set of attributes that will be used in AuthZ decision request and policy evaluation.

The XACML-NRP will also re-use obligations definition in the XACML-Grid profile and extends it to the proposed Reference Model for Obligation Handling (OHRM).

Note:
-------

---

<sup>1</sup> Phosphorus WP4 Wiki link - <http://www.ist-phosphorus.eu/wiki/images/c/c4/Draft-interop-xacml-nrp-profile-01.doc>

<b>Content</b>		
<b>1 Introduction</b>		<b>2</b>
<b>2 Access Control in NRP – Basic Use Cases</b>		<b>2</b>
<b>3 Network topology formats used in multidomain NRP</b>		<b>3</b>
3.1 Phosphorus WP1 topology definition		3
3.2 NDL by UvA and OGF		5
3.3 OSCARS topology description format		6
<b>4 Attributes used for Authorisation and XACML policy definition</b>		<b>7</b>
4.1 Attributes namespace		7
4.2 Network or Resource related attributes		7
4.3 Subject related attributes		8
4.4 Action related attributes		9
4.5 Environment related attributes		10
<b>5 Obligations used in NRP</b>		<b>10</b>
5.1 Policy obligations as policy enforcement mechanism		10
5.2 Intradomain network/VLAN mapping		10
5.3 Network user identity mapping Obligations		10
5.4 Usability and accounting Obligations		11
<b>6 Policy Expression conventions</b>		<b>11</b>
6.1 Policy identification and policy resolution		11
6.1.1 General suggestions		11
6.1.2 Policy resolution convention in the GAAA-TK library		12
6.1.3 Policy identification		13
<b>Appendix A - XACML-NRP profile attributes and policy expression conventions used in Phosphorus project</b>		<b>15</b>
<b>Appendix B - Topology description examples</b>		<b>20</b>
<b>Appendix C - XACML Identifiers (as defined in XACML2.0 specification [XACML2.0])</b>		<b>33</b>
<b>Appendix D - XACML-Grid profile Identifiers [XACML-Grid]</b>		<b>38</b>

## 1 Introduction

The document starts from the short overview of the proposed (in the Phosphorus project) AuthZ infrastructure for multidomain Network Resource Provisioning (NRP), in particular for high-performance dedicated optical networks.

Summary of the proposed design suggestions and solutions for the XACML-NRP profile definition and implementation:

- 1) Network topology formats analysis and definition of initial basic set of attributes for XACML policy definition.
- 2) Definition of an initial set of attributes and policy obligations needed to support general NRP model and layered Phosphorus Network Service Plane (NSP) architecture that should allow integration of different Network Resource Provisioning Systems (NRPS)
- 3) Definition of an initial set of Obligations Handling Reference Model (OHRM) definition and implementation suggestions.
- 4) XACML\_NRP policy examples and conformance test definition.

Examples of current uses in the Phosphorus project are provided in the Appendix A. This is supported by current implementation of the GAAA-TK library (Java based).

## 2 Access Control in NRP – Basic Use Cases

Access control system and infrastructure protect the resource to allow/ensure that only authorised users can have access or execute specific actions on the resource.

In general, the access control policy comprises of rules and conditions that specify what user with what attributes may access or execute what action on the resource with what attributes.

Two particular use cases for access control in Network Resource Provisioning (NRP) can be expressed in a simple narrative form:

**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".**

The following assumptions are made to satisfy the two above use cases and to ensure effective management of policies, user and resource identities and attributes:

- 1) Users and resources are described/identified by their unique ID's and may have also assigned attributes, which for the user may include such attributes as user group, role, or federation, and for the resource may include such attributes as domain/subdomain, resource type, level of service;
- 2) users and resources (domains and endpoints) may be organised/associated into administrative and or security domains or federations, i.e. a user and a resource can be a member of one or multiple associations;
- 3) different domains and endpoints participating in network connection (for which the authorisation is requested) may belong to different federations or security associations;
- 4) 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.
- 5) User authentication may be resulted in the following:
  - a. service or process session initiation;
  - b. release of the user attributes or credentials;
- 6) depending on the user attributes (federations, groups, roles) the user can be assigned specific level of service;
- 7) simple policy format will contain rules that express conditions what user attributes are required to access the resource with specific attributes or execute a specific action on the resource with specific attributes.

### **3 Network topology formats used in multidomain NRP**

Rationale for the topology format:

- Topology format should provide necessary information about the network resource to allow consistent policy evaluation, and vice versa the policy format may be defined but the network topology to which the policy is applied.
- Topology semantics will define the resource attributes semantics, and vice versa.

#### **3.1 Phosphorus WP1 topology definition**

The network resource description includes the following attributes:

- domainId
- relationship or subdomain
- VLAN
- TNA and TNA prefix
- Link parameters average delay and maximum bandwidth
- ReservationEPR as an attribute that may directly or indirectly define the resource federation or security/administrative domain

This information is presented in the XML based network topology description:

## Example 1

```
<ns4:Domains>
  <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">SURFnet</ns3:DomainId>
  <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
  <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">8279</ns3:SequenceNumber>
  <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">SURFnet DRAC domain</ns3:Description>
  <ns3:ReservationEPR
xmlns:ns3="http://ist_phosphorus.eu/nsp">http://10.1.4.1:8080/DracNRPS_WSRF/services/Reservation</n
s3:ReservationEPR>
  <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">10.4.0.0/16</ns3:TNAPrefix>
</ns4:Domains>
```

## Example 2

```
<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/MyServ
ice</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/MySer
vice</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>
```

## Example 3

```
<ns4:getEndpointsResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/websevice/topology">
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.8.1.2</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Endpoint2</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">CRC_To_Viola</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">crc</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1250</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.8.1.4</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Endpoint4</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">CRC_To_SURFnet</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">crc</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1250</ns3:Bandwidth>
  </ns4:Endpoints>
</ns4:getEndpointsResponse>
```

## Example 4

```
<ns4:getLinksResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/websevice/topology">
  <ns4:Link>
    <ns4:SourceEndpoint>10.8.1.4</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.4.1.2</ns4:DestinationEndpoint>
    <ns4:Name>VLAN948</ns4:Name>
    <ns4:Description>crc-SURFnet interdomain link "VLAN948"</ns4:Description>
  </ns4:Link>
  <ns4:Link>
    <ns4:SourceEndpoint>10.7.3.2</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.4.1.1</ns4:DestinationEndpoint>
    <ns4:Name>VLAN947</ns4:Name>
    <ns4:Description>viola-SURFnet interdomain link "VLAN947"</ns4:Description>
  </ns4:Link>
</ns4:getLinksResponse>
```

## 3.2 NDL by UvA and OGF

NDL topology description uses RDF format for describing relations between network entity and its property. The following attributes or properties are specified:

- Device identified by the name
- Location describing domain
- Interface
- port
- link
- bandwidth

### Example 1

```
<!-- 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:501/3"/>

  <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 2

```
<rdf:Description rdf:about="">
  <!-- meta data on this document itself -->
  <rdfs:label xml:lang="en">Configuration of Speculaas</rdfs:label>
  <dc:title xml:lang="en">Configuration of Speculaas</dc:title>
  <dc:description xml:lang="en">Configuration of the Speculaas switch at Netherlight. This
file is semi-dynamically generated by a cron job that logs in the devices and retrieves all
information. You should expect this data to be stale for about 5 minutes. If you really need real-
time data, then don't use NDL, but another mechanism (e.g. a routing protocol).</dc:description>
  <dc:publisher xml:lang="en">glimmerglassconfig.py script on
ndl.uva.netherlight.nl</dc:publisher>
  <dcterms:issued>2007-01-31</dcterms:issued>
  <dcterms:modified>2007-12-12T15:17:11+0100</dcterms:modified>
</rdf:Description>

<ndl:Device rdf:about="http://speculaas.uva.netherlight.nl#Speculaas">
  <rdfs:label>Speculaas</rdfs:label>
  <dc:description xml:lang="en">Speculaas Glimmerglass OXC</dc:description>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf01"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf02"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf03"/>

  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf19"/>
  <capability:hasSwitchMatrix>
  <capability:SwitchMatrix rdf:about="http://speculaas.uva.netherlight.nl#FiberSwitchMatrix">
    <capability:hasSwitchingCapability
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement" />
    <capability:hasSwappingCapability
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement" />
    <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf01"/>
    <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf02"/>

    <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf12"/>
  </capability:SwitchMatrix>
```

```

    </capability:hasSwitchMatrix>
</ndl:Device>

<ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf01">
  <rdf:type rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement" />
  <!-- static FiberInterface -->
  <rdfs:label>1</rdfs:label>
  <dc:description xml:lang="en">Rembrandt0 (10GE)</dc:description>
  <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
3.29</wdm:ingressPowerLevel>
  <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
53.03</wdm:egressPowerLevel>
</ndl:Interface>

<ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf02">
  <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement" />
  <!-- static FiberInterface -->
  <rdfs:label>2</rdfs:label>
  <dc:description xml:lang="en">Rembrandt1 (10GE)</dc:description>
  <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
3.76</wdm:ingressPowerLevel>
  <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
52.22</wdm:egressPowerLevel>
</ndl:Interface>

```

### 3.3 OSCARS topology description format

OSCARS project uses topology description in a form of XML file that includes set of end points srcEndpoint and destEndpoint together with the path description as the list of connecting hops/links.

Endpoints and links are identified by ID's in a form of URN consisting of the following parts:

- Domain (or LAN)
- Node
- Port
- link

Example of the OSCARS resource URN:

```
urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2
```

#### Example 1

```

<!-- 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>

```

## 4 Attributes used for Authorisation and XACML policy definition

### 4.1 Attributes namespace

The XACML-NRP attribute profile will use AuthZ interoperability namespace of URL style “http://authz-interop.org/” introduced in the recently released XACML-Grid profile:

http://authz-interop.org/nrp/xacml

Note: Alternatively it can be considered the URN-style for proprietary or potentially to be registered namespace:

x-urn:authz-interop:nrp:xacml

### 4.2 Network or Resource related attributes

Network related attributes allow building policy depending on the network topology or other network characteristics.

Network related attributes are considered as a part of the XACML Resource definition.

The following resource/network related attributes can be specified and used for authorisation:

- 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

Attribute name	Attribute ID	Full XACML attributeld semantics (ns-prefix = http://authz-interop.org/nrp/xacml)	Notes
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	Consider relation between TNA, EPR and node
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	Consider splitting on two limits:  bandwidth/(min-limit, max-limit)
Resource type	resource-type	{ns-prefix} /resource/resource-type ({ns-prefix} /resource/device)	Resource type may be considered as part of the resource ID by adding "resource-type/{type}" prefix/selector
Resource federation	federation	{ns-prefix} /resource/federation	This attribute can be considered as common for Resource and Subject because both of them can be members of the same federation of VO

The later versions of this document will identify a number of enumerated values for attributes that can be enumerated, such as Resource type (e.g. nsp, nrps, mss) or typically have limited number of the pre-configured values such project related federations/VO, or trusted authorities.

### 4.3 Subject related attributes

Subject related attributes allow building policy depending on the properties of the request Subject or user.

Subject related attributes are considered as a part of the XACML Subject definition.

The following subject related attributes can be specified:

- Subject ID
- Subject confirmation that contains AuthN assertion/token or other attribute confirming subject's ID by trusted AuthN authority
- Subject Role
- Subject Group
- Subject Aederation (e.g., Virtual Organisation, or Shibboleth AAI federation) or domain
- Subject context that can provide additional information about the Subject other than Subject federation e.g. such as Session ID, or project/experiment name

Attribute name	Attribute ID	Full XACML attributeld semantics (ns-prefix = http://authz-interop.org/nrp/xacml)	Notes
Subject ID	subject-id	{ns-prefix} /subject/subject-id	Consider using standard XACML attribute ID:  urn:oasis:names:tc:xacml:1.0:subject:subject-id
Subject confirmation	subject-confdata	{ns-prefix} /subject/subject-confdata	

Subject federation	federation	{ns-prefix} /subject/federation	This attribute should be considered as similar to the "subject-vo" in XACML-Grid profile if network domain or endpoint are members of a VO
Subject group	subject-group	{ns-prefix} /subject/subject-group	
Subject role	subject-role	{ns-prefix} /subject/subject-role	Consider relation between TNA, EPR and node
Subject Context	subject-context	{ns-prefix} /subject/subject-context	

Subject attributes are provided as Subject credentials which depending on user client implementation and middleware may take a form of X.509 public key and attribute certificates (PKC, AC), SAML Authentication and Attribute assertions, proprietary AuthN system credentials.

Subject may also use attributes defined in the XACML-Grid profile or attributes originally defined in the XACML and SAML specifications. See Appendix for such candidate attributes.

#### 4.4 Action related attributes

Action related attributes represent a limited number of the specific actions that requesting party can ask to initiate network resource reservation, access or management.

Action related attributes are considered as part of the XACML Action definition.

The following Action related attributes can be specified:

- Action ID
- Action type

Attribute name	Attribute ID	Full XACML attributeld semantics (ns-prefix = http://authz-interop.org/nrp/xacml)	Notes
Action ID	action-id	{ns-prefix} /action/action-id	Consider using standard XACML attribute ID:  urn:oasis:names:tc:xacml:1.0:action:action-id
Action type	action-type	{ns-prefix} /action/action-type/{value}	This type of attribute identifier is used only together with the enumerated action identifier

List of action type enumerated values:

Attribute name	Enumerated value	XACML attribute value (ns-prefix = http://authz-interop.org/nrp/xacml)	Notes
----------------	------------------	--	-------

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

#### 4.5 Environment related attributes

Environment related attributes allow providing additional information for policy definition and evaluation.

Environment related attributes are considered as part of the XACML Environment definition.

There is no specific Environment attributes identified for XACML-NRP profile at this moment. Refer to Appendix for list of the Environment attributes specified in XACML2.0 specification and XACML-Grid profile.

## 5 Obligations used in NRP

### 5.1 Policy obligations as policy enforcement mechanism

Policy obligation is one of the authorisation policy enforcement mechanisms that allows adding AuthZ decision enforcement components that can not be defined in the policy at the moment of making policy decision by the PDP, or may not be known to the PDP or policy administrator/writer

Suggested functionality that can be achieved with using obligations includes but not limited to:

- Intradomain network/VLAN mapping for cross-domain connections, that can be used to map external/interdomain border links/TNA's to internal VLAN and sub-network
- Account mapping
- 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/quota

### 5.2 Intradomain network/VLAN mapping

This may be needed for defining specific intradomain mapping of cross-domain connections depending on specific reservation, path or user attributes.

### 5.3 Network user identity mapping Obligations

This obligation is returned by the PDP in case of positive decision with instruction to what type of or a specific pool account the user identity should be mapped when accessing a requested network resource.

The need of account mapping may exist in cases when domain based Network Resource Provisioning Systems (NRPS) have pre-installed/built-in pool accounts to which are different types or quality of service are assigned. In such situation authorised user need to use one of such accounts, e.g. "silver", "golden", "platinum". A number of different individual accounts of the same type may be limited, consequently a dynamically assigned account should be selected from the pool of available or free accounts. Such dynamic

account assignment can not be specified in the typically stateless policy and cannot be done by PDP. However, the access control policy may contain instruction to PEP to do such mapping.

More details and suggestions about identity mapping obligation will be provided in the next version of the document.

## 5.4 Usability and accounting Obligations

Usability and accounting obligations allow that some usability attributes (e.g. number of downloads, total time of using network resource, amount of data transferred) assigned or accounting instruction are applied to the specific request decision.

More details and suggestions about usability and accounting obligation will be provided in the next version of the document.

## 6 Policy Expression conventions

This section will discuss requirements to and describe the conformance test to ensure interoperability of the potentially different XACML-NRP implementations.

The simple policy example for the specified at the beginning use case 1 will evaluate the request to NSP system for one of actions "create-path, activate-path, cancel, access" from the user with attributes "admin, researcher, professor, or student". Access control table has the following view:

Access Control Table for simple NSP AuthZ policy

Roles	Admin	Researcher	Professor	Student
Create-Path	1	1	0	0
Activate-Path	1	1	1	0
Cancel	1	0	0	0
Access	1	1	1	1

The example in the Appendix A illustrates how such access control table can implemented in XACML using the proposed attributes definition.

### 6.1 Policy identification and policy resolution

#### 6.1.1 General suggestions

When evaluating AuthZ request the ContextHandler or PDP (refer to [??] for the generic AuthZ service architecture and basic AuthZ service components participation in AuthZ) need to find/select an applicable policy. This is typically done based on the request parameters such as Resource or Subject attributes.

The policy selecting/finding comprises of two steps: policy resolution and policy retrieval. Policy resolution means extracting such information from the AuthZ request that can be used for further policy selection in the storage/repository. Based on this information, a repository request or query can be constructed to retrieve necessary policy.

Note, it is a SunXACML implementation convention that only one Policy or PolicySet should be supplied to PDP for evaluation, and only one component Policy must be selected if using PolicySet.

The following components of the XACML-NRP profile can be used for policy resolution:

- a) resource ID and resource attributes;
- b) subject attributes defining context in which the request should evaluated, e.g. project or VO (this information is typically a part of the subject attributes);
- c) attributes and policy profile namespace, which can actually be a part of the resource ID if expressed in Fully Qualified Attribute Name format (FQAN format).

Depending on the policy storage/repository implementation, the following components can be used for policy identification:

- a) policy file name and directory, if policy is stored as a file;
- b) PolicyId attribute of the PolicySet or Policy element;
- c) policy Target element that can include any of Subject, Resource, Action, Environment elements.

Although using basically different ways of storing policies, the first case and second identification methods can be based on similar approach to composing PolicyId attribute and (defining) policy file location path. When using third option, the policy repository should be capable to query policy database by the policy Target content.

### 6.1.2 Policy resolution convention in the GAAA-TK library

Two components are used for policy resolution in GAAA-TK library profile for Network Resource Provisioning (GAAA-NRP):

- ResourceId expressed in the URL-style URI format, actually specifying the resource FQAN;
- Subject context (SubjectCtx) that specifies subject (and resource) association (e.g., VO, experiment, or project )

General ResourceId expression format:

```
<<ns-type>><Realm>/<ns-domain>/(<device-type> | <resource-context>)/<variables-name-value-pairs>
```

Examples:

URL style:

```
http://testbed.ist-phosphorus.eu/viola/nsp/source=10.1.1.3/target=10.3.1.3
http://testbed.ist-phosphorus.eu/resource-type/harmony
http://testbed.ist-phosphorus.eu/resource-context/phosphorus
```

where

```
"http://" - URL style namespace identifier;
"testbed.ist-phosphorus.eu" - namespace realm;
"viola", "resource-type", "resource-context" - namespace domain;
"nsp", "harmony", "phosphorus" - device type or resource context;
"source", "target" - device variable presented in a form of "name-value".
```

Note: quotation marks are not allowed in URI string.

The same identifier strings expressed in URN style will use URN specific prefix "x-urn:authz-interop:nrp:resource-id" (or its shorter option "x-urn:nrp:resource-id"):

URN style:

```
x-urn:authz-interop:nrp:resource-id:testbed.ist-
phosphorus.eu:viola:nsp:source=10.1.1.3;target=10.3.1.3
x-urn:authz-interop:nrp:resource-id:testbed.ist-phosphorus.eu:resource-
type:harmony
x-urn:authz-interop:nrp:resource-id:testbed.ist-phosphorus.eu:resource-
context:phosphorus
```

SubjectCtx can be expressed either in a FQAN format or just contain a simple name without namespace prefixes, e.g.

Demo001, or PhosphorusVO, EGEE-VO, etc.

Given above examples the AuthZ Request containing ResourceId and SubjectCtx attributes will be resolved into the following policy path/files:

```
<<root-dir>>/policy/nrp/testbed.ist-phosphorus.eu/viola-policy-nsp-demo001.xml
<<root-dir>>/policy/nrp/testbed.ist-phosphorus.eu/harmony-policy-demo001.xml
<<root-dir>>/policy/nrp/testbed.ist-phosphorus.eu/phosphorus-policy-demo001.xml
```

### 6.1.3 Policy identification

It is suggested that the PolicyId or PolicySetId is created in the same way using typical for URL/URN style conventions:

```
PolicyId = <<url-namespace-prefix/>>testbed.ist-phosphorus.eu/viola/harmony/demo001/policy
```

```
PolicyId = <<urn-namespace-prefix:>>testbed.ist-phosphorus.eu:viola:harmony:demo001:policy
```

where

```
<<namespace-prefix>> - can be dropped;
```

```
namespace-prefix = http://authz-interop.org/nrp/xacml
```

```
or namespace-prefix = x-urn:authz-interop.org:nrp:xacml
```

Example PolicyId expression:

URL style:

```
PolicyId = http://authz-interop.org/nrp/xacml/testbed.ist-phosphorus.eu/phosphorus/demo001/policy
```

```
PolicyId = http://testbed.ist-phosphorus.eu/viola/harmony/demo001/policy
```

```
PolicyId = http://testbed.ist-phosphorus.eu/phosphorus/demo001/policy
```

URN style:

```
PolicyId = x-urn:authz-interop.org:nrp:testbed.ist-phosphorus.eu:viola:harmony:demo001:policy
```

```
PolicyId = x-urn:authz-interop.org:nrp:testbed.ist-phosphorus.eu:phosphorus:demo001:policy
```

## References

- [1] An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids: (OSG link - <http://cd-docdb.fnal.gov/cgi-bin/ShowDocument?docid=2685>, EGEE link - <https://edms.cern.ch/document/929867/1>)
- [2] SAML–XACML Authorisation Interface and XACML Obligations Handling. Work in progress. Draft version 0.3, April 29, 2008. - <http://staff.science.uva.nl/~demch/projects/aaauthreach/draft-authz-saml-xacml-obligations-03.pdf>
- [3] *eXtensible Access Control Markup Language (XACML) Version 2.0*, OASIS Standard, 1 February 2005. [Online]. Available: [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)
- [4] *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS Standard, 15 March 2005. [Online]. Available: <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [5] SAML 2.0 Profile of XACML 2.0, Version 2. Working Draft 2, 26 June 2006. [Online]. Available: <http://docs.oasis-open.org/xacml/2.0/xacml-2.0-profile-saml2.0-v2.zip>
- [6] "Multiple resource profile of XACML 2.0", OASIS Standard, 1 February 2005, available from [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-mult-profile-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-mult-profile-spec-os.pdf)
- [7] "Hierarchical resource profile of XACML 2.0", OASIS Standard, 1 February 2005, available from [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-hier-profile-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-hier-profile-spec-os.pdf)
- [8] *Core and hierarchical role based access control (RBAC) profile of XACML v2.0*, OASIS Standard, 1 February 2005. [Online]. Available: [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-rbac-profile1-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf)
- [9] GFD.38 Conceptual Grid Authorization Framework and Classification. M. Lorch, B. Cowles, R. Baker, L. Gommans, P. Madsen, A. McNab, L. Ramakrishnan, K. Sankar, D. Skow, M. Thompson - <http://www.ggf.org/documents/GWD-I-E/GFD-I.038.pdf>
- [10] RFC2748: The COPS (Common Open Policy Service) Protocol, Edited Durham, D., January 2000. - <http://www.ietf.org/rfc/rfc2748.txt>
- [11] RFC2753: A Framework for Policy-based Admission Control, January 2000. - <http://www.ietf.org/rfc/rfc2753.txt>
- [12] Phosphorus Project Deliverable D4.1 "AAA Architectures for multi-domain optical networking scenario's". - <http://www.ist-phosphorus.eu/files/deliverables/Phosphorus-deliverable-D4.1.pdf>
- [13] Deliverable DJ5.2.2: GÉANT2 Authorisation and Authentication Infrastructure (AAI) Architecture. - <http://www.geant2.net/upload/pdf/GN2-05-192v6.pdf>
- [14] Deliverable DJ5.2.3,2: Best Practice Guide - AAI Cookbook - Second Edition Guidelines for Connecting to the eduGAIN AA Infrastructure. - [http://www.geant2.net/upload/pdf/GN2-07-023v4-DJ5-2-3\\_2\\_Best\\_Practice\\_Guide-AAI\\_Cookbook-Second\\_Edition.pdf](http://www.geant2.net/upload/pdf/GN2-07-023v4-DJ5-2-3_2_Best_Practice_Guide-AAI_Cookbook-Second_Edition.pdf)

## Appendix A - XACML-NRP profile attributes and policy expression conventions used in Phosphorus project

### A.1 Attribute expression conventions

Current XACML-NRP profile implementation in the Phosphorus project is supported by the GAAA-TK library.

Information provided in the AuthZ request to PEP-PDP contains information about Resource, Subject, Action, and optionally Environment.

#### Resource attributes

Currently the Resource element contains one attribute ResourceId (attribute identifier “resource-id”) in the form of URI string that includes the network resource identifier and a list or parameter used for policy-based request evaluation.

The following ResourceId formats are supported:

a) `http://testbed.ist-phosphorus.eu/{domain}/{device | service}/{parameters}`

Example: `http://testbed.ist-phosphorus.eu/viola/nsp/source=10.7.12.2/target=10.3.17.3,`

where

`http://testbed.ist-phosphorus.eu/viola/nsp` - resource identifier

`source=10.7.12.2/target=10.3.17.3` – resource parameters

b) `http://testbed.ist-phosphorus.eu/resource-type/{resource-type-name}`

Example: `http://testbed.ist-phosphorus.eu/resource-type/ nsp`

c) `http://testbed.ist-phosphorus.eu/resource-context/{(project | association) name}` (optional)

Example: `http://testbed.ist-phosphorus.eu/resource-context/phosphorus`

#### Subject attributes

The Resource element contains the following attributes:

a) SubjectId (attribute identifier “subject-id”) – subject identifier in RFC822 (email) or X.521 format (must be the same as used in the SubjectConfirmatioData)

Example: `WHO740@users.testbed.ist-phosphorus.eu`

b) SubjectConfirmatioData (attribute identifier “subject-confdata”) – Authentication assertion or token provided by the trusted AuthN service (can be also SAML AuthN Assertion), or crypto-string provided local AuthN service.

c) SubjectRole (attribute identifier “subject-role”) – subject role, currently supporting single attribute.

Future GAAA-TK release will support coma-separated list of roles, SAML Attribute assertion and VOMS Attribute Certificate

d) SubjectContext (attribute identifier "subject-context") – this attribute is used for providing additional information about user (and resource) association like VO, Project, experiment/job.

Potentially can be extended to provide instant reservation context for dynamically configured AuthZ service.

## A.2 XACML policy and messages examples

### A.2.1. Simple policy example for integration with Phosphorus WP1 NSP/Harmony Network Resource Provisioning System (NRP)

Defines rules to permit selected actions "create-path, activate-path, cancel, access" from a user with attributes "admin, researcher, professor, student" to a specific resource for which the policy is defined.

```
<Policy PolicyId="http://authz-interop.org/AAA/xacml/policy/nsp/demo001"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
  <Description>Permit actions for Phosphorus testbed 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://testbed.ist-phosphorus.eu/viola/nsp</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="http://authz-interop.org/AAA/xacml/policy/viola/nsp/demo001/action-type/create-path" 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">create-path</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">admin</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">researcher</AttributeValue>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">professor</AttributeValue>
      </Apply>
      <SubjectAttributeDesignator AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-role" DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Condition>
  </Rule>
  <Rule RuleId="http://authz-interop.org/AAA/xacml/policy/viola/nsp/demo001/action-type/activate-path" Effect="Permit">
    <Target>
      <Subjects>
        <AnySubject/>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
    </Target>
```

```

</Resources>
<Actions>
  <Action>
    <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">activate-
path</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">researcher</AttributeValue>
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">professor</AttributeValue>
  </Apply>
  <SubjectAttributeDesignator AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-
role" DataType="http://www.w3.org/2001/XMLSchema#string" />
</Condition>
</Rule>
<Rule RuleId="http://authz-interop.org/AAA/xacml/policy/viola/nsp/demo001/action-type/cancel"
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">cancel</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">admin</AttributeValue>
    </Apply>
    <SubjectAttributeDesignator AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-
role" DataType="http://www.w3.org/2001/XMLSchema#string" />
  </Condition>
</Rule>
<Rule RuleId="http://authz-interop.org/AAA/xacml/policy/viola/nsp/demo001/action-type/access"
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">access</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">admin</AttributeValue>
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">professor</AttributeValue>
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">researcher</AttributeValue>
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">student</AttributeValue>
    </Apply>

```

```

    <SubjectAttributeDesignator AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-
role" DataType="http://www.w3.org/2001/XMLSchema#string" />
  </Condition>
</Rule>
</Policy>
DataType="http://www.w3.org/2001/XMLSchema#string">researcher</AttributeValue>

```

2) Request message sent to XACML PDP that contains the following attributes

Subject related attributes

- subject-id
- subject-confdata
- subject-role
- subject-context

and Resource related attributes that currently contains only

- ResourceId URI string

ResourceId substring "" and Subject-context are used for policy (file) selection.

```

<Request>
  <Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
    <Attribute AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-confdata"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="x-urn:aaa:xacml:AttributeIssuer"
IssueInstant="2008-06-20T03:07:42.078000000+02:00">
      <AttributeValue>IGhA1lvwa8bUktYhuU9que+d4XLUVJFHrtDC/OE3UilbxtmCxLldw==
    </AttributeValue>
  </Attribute>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="x-urn:aaa:xacml:AttributeIssuer"
IssueInstant="2008-06-20T03:07:42.078000000+02:00">
      <AttributeValue>WHO740@users.testbed.ist-phosphorus.eu</AttributeValue>
    </Attribute>
  <Attribute AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-context"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="x-urn:aaa:xacml:AttributeIssuer"
IssueInstant="2008-06-20T03:07:42.078000000+02:00">
      <AttributeValue>demo001</AttributeValue>
    </Attribute>
  <Attribute AttributeId="http://authz-interop.org/AAA/xacml/subject/subject-role"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="x-urn:aaa:xacml:AttributeIssuer"
IssueInstant="2008-06-20T03:07:42.078000000+02:00">
      <AttributeValue>researcher</AttributeValue>
    </Attribute>
  </Subject>
<Resource>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI" Issuer="x-urn:aaa:xacml:AttributeIssuer"
IssueInstant="2008-06-20T03:07:42.078000000+02:00">
      <AttributeValue>http://testbed.ist-phosphorus.eu/viola/nsp</AttributeValue>
    </Attribute>
  </Resource>
<Action>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="x-urn:aaa:xacml:AttributeIssuer"
IssueInstant="2008-06-20T03:07:42.078000000+02:00">
      <AttributeValue>create-path</AttributeValue>
    </Attribute>
  </Action>
<Environment>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="x-urn:aaa:xacml:AttributeIssuer"
IssueInstant="2008-06-20T03:07:42.078000000+02:00">
      <AttributeValue>null</AttributeValue>
    </Attribute>
  </Environment>
</Request>

```

## 2) Response message returned by XACML PDP that Decision information “Permit” or “Deny” and related status information

```
<Response>
  <Result ResourceID="http://testbed.ist-phosphorus.eu/viola/nsp">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

### A.2.1. Policy examples using matching functions with regular expressions

#### 1) Regular expression functions

urn:oasis:names:tc:xacml:1.0:function:string-intersection

urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of

urn:oasis:names:tc:xacml:1.0:function:string-union

\* urn:oasis:names:tc:xacml:1.0:function:string-subset

urn:oasis:names:tc:xacml:1.0:function:string-set-equals

\*\*\* urn:oasis:names:tc:xacml:1.0:function:string-regexp-match

\*\* urn:oasis:names:tc:xacml:2.0:function:anyURI-regexp-match

\* urn:oasis:names:tc:xacml:2.0:function:ipAddress-regexp-match

urn:oasis:names:tc:xacml:2.0:function:dnsName-regexp-match M

urn:oasis:names:tc:xacml:2.0:function:rfc822Name-regexp-match

urn:oasis:names:tc:xacml:2.0:function:x500Name-regexp-match

urn:oasis:names:tc:xacml:1.0:function:string-greater-than

urn:oasis:names:tc:xacml:1.0:function:string-greater-than-or-equal

urn:oasis:names:tc:xacml:1.0:function:string-less-than

urn:oasis:names:tc:xacml:1.0:function:string-less-than-or-equal

## Appendix B - Topology description examples

### 1) Phosphorus WP1 NSP topology definition

```
<!-- DOMAIN POINT DESCRIPTION -->

<ns4:getDomainsResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Domains>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">SURFnet</ns3:DomainId>
    <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
    <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">8279</ns3:SequenceNumber>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">SURFnet DRAC domain</ns3:Description>
    <ns3:ReservationEPR
xmlns:ns3="http://ist_phosphorus.eu/nsp">http://10.1.4.1:8080/DracNRPS_WSRF/services/Reservation</n
s3:ReservationEPR>
    <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">10.4.0.0/16</ns3:TNAPrefix>
  </ns4:Domains>
  <ns4:Domains>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">viola</ns3:DomainId>
    <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
    <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">48</ns3:SequenceNumber>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">VIOLA domain (combined
MPLS/GMPLS)</ns3:Description>
    <ns3:ReservationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">http://viola-nsp.cs.uni-
bonn.de:8080/reservation/services/MyService</ns3:ReservationEPR>
    <ns3:TopologyEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">http://viola-nsp.cs.uni-
bonn.de:8080/topology/services/MyService</ns3:TopologyEPR>
    <ns3:NotificationEPR xmlns:ns3="http://ist_phosphorus.eu/nsp">http://viola-nsp.cs.uni-
bonn.de:8080/notification/services/MyService</ns3:NotificationEPR>
    <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">10.7.0.0/16</ns3:TNAPrefix>
  </ns4:Domains>
  <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/MyServ
ice</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/MySer
vice</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>
  <ns4:Domains>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">crc</ns3:DomainId>
    <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
    <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">4343</ns3:SequenceNumber>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">crc Domain controlled by
UCLP</ns3:Description>
    <ns3:ReservationEPR
xmlns:ns3="http://ist_phosphorus.eu/nsp">http://10.1.8.1:8080/nrpsUCLPReservation/services/MyServic
e</ns3:ReservationEPR>
    <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">10.8.1.0/24</ns3:TNAPrefix>
  </ns4:Domains>
  <ns4:Domains>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">i2CAT</ns3:DomainId>
    <ns3:Relationship xmlns:ns3="http://ist_phosphorus.eu/nsp">subdomain</ns3:Relationship>
    <ns3:SequenceNumber xmlns:ns3="http://ist_phosphorus.eu/nsp">69</ns3:SequenceNumber>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">i2CAT UCLP domain</ns3:Description>
    <ns3:ReservationEPR
xmlns:ns3="http://ist_phosphorus.eu/nsp">http://10.1.3.100:8080/nrpsUCLPReservation/services/MyServ
ice</ns3:ReservationEPR>
    <ns3:TNAPrefix xmlns:ns3="http://ist_phosphorus.eu/nsp">10.3.1.0/24</ns3:TNAPrefix>
  </ns4:Domains>
</ns4:getDomainsResponse>

<!-- END POINT DESCRIPTION -->
```

```

<ns4:getEndpointsResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.8.1.2</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Endpoint2</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">CRC_To_Viola</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">crc</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1250</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.8.1.4</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Endpoint4</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">CRC_To_SURFnet</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">crc</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1250</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.8.1.3</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Endpoint3</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">CRC_To_i2CAT</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">crc</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1250</ns3:Bandwidth>
  </ns4:Endpoints>
<!-- LINKS DESCRIPTION -->
<ns4:getLinksResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Link>
    <ns4:SourceEndpoint>10.8.1.4</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.4.1.2</ns4:DestinationEndpoint>
    <ns4:Name>VLAN948</ns4:Name>
    <ns4:Description>crc-SURFnet interdomain link "VLAN948"</ns4:Description>
  </ns4:Link>
  <ns4:Link>
    <ns4:SourceEndpoint>10.7.3.2</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.4.1.1</ns4:DestinationEndpoint>
    <ns4:Name>VLAN947</ns4:Name>
    <ns4:Description>viola-SURFnet interdomain link "VLAN947"</ns4:Description>
  </ns4:Link>
</ns4:getLinksResponse>
<ns4:getEndpointsResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.4.1.1</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Viola1 ENNI Phospho Test
(4/1/3)</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">Viola1 ENNI Phospho Test
(4/1/3)</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">SURFnet</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1000</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.4.1.3</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">i2CAT ENNI Phospho Test
(1/1/3)</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">i2CAT ENNI Phospho Test
(1/1/3)</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">SURFnet</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1000</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.4.1.2</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">CRC ENNI Phospho Test (3/1/3</ns3:Name>
(3/1/3)</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">SURFnet</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1000</ns3:Bandwidth>
  </ns4:Endpoints>
</ns4:getEndpointsResponse>
<ns4:getEndpointsResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.7.3.1</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Augustin2_1</ns3:Name>

```

```

    <ns3:Description
xmlns:ns3="http://ist_phosphorus.eu/nsp">Spc_Augustin_Link1_to_SURFnet</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">viola</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1000</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.7.3.4</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Augustin2_4</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">Spc_Augustin_Link3-to-
PSNC</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">viola</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1000</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.7.2.1</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Juelich2_1</ns3:Name>
    <ns3:Description
xmlns:ns3="http://ist_phosphorus.eu/nsp">Spc_Juelich_Link1_to_SURFnet</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">viola</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1000</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.7.3.2</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">Augustin2_2</ns3:Name>
    <ns3:Description
xmlns:ns3="http://ist_phosphorus.eu/nsp">Spc_Augustin_Link2_to_SURFnet</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">viola</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1000</ns3:Bandwidth>
  </ns4:Endpoints>
</ns4:getEndpointsResponse>

<ns4:getLinksResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Link>
    <ns4:SourceEndpoint>10.8.1.2</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.7.3.4</ns4:DestinationEndpoint>
    <ns4:Name>VLAN978</ns4:Name>
    <ns4:Description>crc-viola interdomain link "VLAN978"</ns4:Description>
  </ns4:Link>
  <ns4:Link>
    <ns4:SourceEndpoint>10.7.3.2</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.4.1.1</ns4:DestinationEndpoint>
    <ns4:Name>VLAN947</ns4:Name>
    <ns4:Description>viola-SURFnet interdomain link "VLAN947"</ns4:Description>
  </ns4:Link>
  <ns4:Link>
    <ns4:SourceEndpoint>10.7.3.1</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.3.1.26</ns4:DestinationEndpoint>
    <ns4:Name>VLAN937</ns4:Name>
    <ns4:Description>viola-i2CAT interdomain link "VLAN937"</ns4:Description>
  </ns4:Link>
</ns4:getLinksResponse>

<ns4:getLinksResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Link>
    <ns4:SourceEndpoint>10.3.1.25</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.8.1.3</ns4:DestinationEndpoint>
    <ns4:Name>VLAN938</ns4:Name>
    <ns4:Description>i2CAT-crc interdomain link "VLAN938"</ns4:Description>
  </ns4:Link>
  <ns4:Link>
    <ns4:SourceEndpoint>10.7.3.1</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.3.1.26</ns4:DestinationEndpoint>
    <ns4:Name>VLAN937</ns4:Name>
    <ns4:Description>viola-i2CAT interdomain link "VLAN937"</ns4:Description>
  </ns4:Link>
</ns4:getLinksResponse>

<ns4:getLinksResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Link>
    <ns4:SourceEndpoint>10.8.1.2</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.7.3.4</ns4:DestinationEndpoint>
    <ns4:Name>VLAN978</ns4:Name>
    <ns4:Description>crc-viola interdomain link "VLAN978"</ns4:Description>
  </ns4:Link>
  <ns4:Link>
    <ns4:SourceEndpoint>10.3.1.25</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.8.1.3</ns4:DestinationEndpoint>

```

```

    <ns4:Name>VLAN938</ns4:Name>
    <ns4:Description>i2CAT-crc interdomain link "VLAN938"</ns4:Description>
  </ns4:Link>
  <ns4:Link>
    <ns4:SourceEndpoint>10.8.1.4</ns4:SourceEndpoint>
    <ns4:DestinationEndpoint>10.4.1.2</ns4:DestinationEndpoint>
    <ns4:Name>VLAN948</ns4:Name>
    <ns4:Description>crc-SURFnet interdomain link "VLAN948"</ns4:Description>
  </ns4:Link>
</ns4:getLinksResponse>

<ns4:getEndpointsResponse xmlns:ns4="http://ist_phosphorus.eu/nsp/webservice/topology">
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.3.1.26</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">oci6-optera2</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">Port facing VIOLA (port 7 of the
switch - VLAN 937)</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">i2CAT</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1250</ns3:Bandwidth>
  </ns4:Endpoints>
  <ns4:Endpoints>
    <ns3:EndpointId xmlns:ns3="http://ist_phosphorus.eu/nsp">10.3.1.25</ns3:EndpointId>
    <ns3:Name xmlns:ns3="http://ist_phosphorus.eu/nsp">oci5-optera2</ns3:Name>
    <ns3:Description xmlns:ns3="http://ist_phosphorus.eu/nsp">Port facing CRC (port 6 of the
switch - VLAN 938)</ns3:Description>
    <ns3:Interface xmlns:ns3="http://ist_phosphorus.eu/nsp">border</ns3:Interface>
    <ns3:DomainId xmlns:ns3="http://ist_phosphorus.eu/nsp">i2CAT</ns3:DomainId>
    <ns3:Bandwidth xmlns:ns3="http://ist_phosphorus.eu/nsp">1250</ns3:Bandwidth>
  </ns4:Endpoints>
</ns4:getEndpointsResponse>

```

## 2) NDL by UvA and OGF

```

<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:ndl="http://www.science.uva.nl/research/sne/ndl#">

  <!-- Description of Netherlight -->
  <ndl:Location rdf:about="#Netherlight">
    <ndl:name>Netherlight Optical Exchange</ndl:name>
  </ndl:Location>

  <!-- TDM3.amsterdaml.netherlight.net -->
  <ndl:Device rdf:about="#tdm3.amsterdaml.netherlight.net">
    <ndl:name>tdm3.amsterdaml.netherlight.net</ndl:name>
    <ndl:locatedAt rdf:resource="#amsterdaml.netherlight.net"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:501/1"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:501/2"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:501/3"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:501/4"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:503/1"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:503/2"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:503/3"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:503/4"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:504/1"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:504/2"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:504/3"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:504/4"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:505/1"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:505/2"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:505/3"/>
    <ndl:hasInterface rdf:resource="#tdm3.amsterdaml.netherlight.net:505/4"/>
  </ndl:Device>

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

```

```

    <ndl:connectedTo rdf:resource="#tdm2.amsterdam1.netherlight.net:6/1"/>
    <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:501/4">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS501/4</ndl:name>
  <ndl:connectedTo rdf:resource="#UvA-Force10:4/0"/>
  <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:503/1">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS503/1</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm1.Prahal:6/1"/>
  <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:503/2">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS503/2</ndl:name>
  <ndl:connectedTo rdf:resource="#Starlight-HDXc:502/2"/>
  <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:503/3">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS503/3</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm1.geneval.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:503/4">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS503/4</ndl:name>
  <ndl:connectedTo rdf:resource="#UvA-Force10:4/1"/>
  <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:504/1">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS504/1</ndl:name>
  <ndl:connectedTo rdf:resource="#Manlan-HDXc:503/4"/>
  <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:504/2">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS504/2</ndl:name>
  <ndl:connectedTo rdf:resource="#GEANT-M160:0/0"/>
  <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:504/3">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS504/3</ndl:name>
  <ndl:connectedTo rdf:resource="#Manlan-HDXc:504/1"/>
  <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:504/4">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS504/4</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm1.geneval.netherlight.net:6/1"/>
  <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:505/1">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS505/1</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm1.amsterdam1.netherlight.net:6/1"/>
  <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:505/2">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS505/2</ndl:name>
  <ndl:connectedTo rdf:resource="#Manlan-HDXc:503/2"/>
  <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:505/3">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS505/3</ndl:name>
  <ndl:connectedTo rdf:resource="#Starlight-HDXc:503/2"/>
  <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:505/4">
  <ndl:name>tdm3.amsterdam1.netherlight.net:POS505/4</ndl:name>
  <ndl:connectedTo rdf:resource="#????:0/0"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
</ndl:Interface>

<!-- TDM4.amsterdam1 -->
<ndl:Device rdf:about="#tdm4.amsterdam1.netherlight.net">
  <ndl:name>tdm4.amsterdam1.netherlight.net</ndl:name>
  <ndl:locatedAt rdf:resource="#amsterdam1.netherlight.net"/>
  <ndl:hasInterface rdf:resource="#tdm4.amsterdam1.netherlight.net:5/1"/>
</ndl:Device>
<ndl:Interface rdf:about="#tdm4.amsterdam1.netherlight.net:5/1">
  <ndl:name>tdm4.amsterdam1.netherlight.net:POS5/1</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm3.amsterdam1.netherlight.net:501/1"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
</ndl:Interface>

```

```

<!-- TDM1.amsterdam1 -->
<ndl:Device rdf:about="#tdml.amsterdam1.netherlight.net">
  <ndl:name>tdml.amsterdam1.netherlight.net</ndl:name>
  <ndl:locatedAt rdf:resource="#amsterdam1.netherlight.net"/>
  <ndl:hasInterface rdf:resource="#tdml.amsterdam1.netherlight.net:5/1"/>
  <ndl:hasInterface rdf:resource="#tdml.amsterdam1.netherlight.net:6/1"/>
  <ndl:hasInterface rdf:resource="#tdml.amsterdam1.netherlight.net:12/1"/>
  <ndl:hasInterface rdf:resource="#tdml.amsterdam1.netherlight.net:16/1"/>
  <ndl:hasInterface rdf:resource="#tdml.amsterdam1.netherlight.net:17/1"/>
</ndl:Device>
<ndl:Interface rdf:about="#tdml.amsterdam1.netherlight.net:5/1">
  <ndl:name>tdml.amsterdam1.netherlight.net:POS5/1</ndl:name>
  <ndl:connectedTo rdf:resource="#RIPN-Gloriad:0/0"/>
  <capacity rdf:resource="#OC12"/>
</ndl:Interface>
<ndl:Interface rdf:about="#tdml.amsterdam1.netherlight.net:6/1">
  <ndl:name>tdml.amsterdam1.netherlight.net:POS6/1</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm3.amsterdam1.netherlight.net:505/1"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
</ndl:Interface>
<ndl:Interface rdf:about="#tdml.amsterdam1.netherlight.net:12/1">
  <ndl:name>tdml.amsterdam1.netherlight.net:POS12/1</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm3.amsterdam1.netherlight.net:501/2"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
</ndl:Interface>
<ndl:Interface rdf:about="#tdml.amsterdam1.netherlight.net:16/1">
  <ndl:name>tdml.amsterdam1.netherlight.net:POS16/1</ndl:name>
  <ndl:connectedTo rdf:resource="#br1.amsterdam1.surf.net:5/1"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">3E+8</ndl:capacity>
</ndl:Interface>
<ndl:Interface rdf:about="#tdml.amsterdam1.netherlight.net:17/1">
  <ndl:name>tdml.amsterdam1.netherlight.net:POS17/1</ndl:name>
  <ndl:connectedTo rdf:resource="#Nordunet:6/1"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">3E+8</ndl:capacity>
</ndl:Interface>

<!-- TDM1.geneval -->
<ndl:Device rdf:about="#tdml.geneval.netherlight.net">
  <ndl:name>tdml.geneval.netherlight.net</ndl:name>
  <ndl:locatedAt rdf:resource="#geneval.netherlight.net"/>
  <ndl:hasInterface rdf:resource="#tdml.geneval.netherlight.net:5/1"/>
  <ndl:hasInterface rdf:resource="#tdml.geneval.netherlight.net:6/1"/>
  <ndl:hasInterface rdf:resource="#tdml.geneval.netherlight.net:13/1"/>
</ndl:Device>
<ndl:Interface rdf:about="#tdml.geneval.netherlight.net:5/1">
  <ndl:name>tdml.geneval.netherlight.net:POS5/1</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm3.amsterdam1.netherlight.net:503/3"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
</ndl:Interface>
<ndl:Interface rdf:about="#tdml.geneval.netherlight.net:6/1">
  <ndl:name>tdml.geneval.netherlight.net:POS6/1</ndl:name>
  <ndl:connectedTo rdf:resource="#tdm3.amsterdam1.netherlight.net:504/4"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
</ndl:Interface>
<ndl:Interface rdf:about="#tdml.geneval.netherlight.net:13/1">
  <ndl:name>tdml.geneval.netherlight.net:POS13/1</ndl:name>
  <ndl:connectedTo rdf:resource="#Forcel0-Cern:0/0"/>
  <ndl:capacity rdf:datatype="http://www.w3.org/2001/XMLSchema#float">1.2E+9</ndl:capacity>
</ndl:Interface>
</rdf:RDF>

```

```

<?xml version="1.0" encoding="UTF-8"?>
<rdf:RDF
  xmlns:ndl="http://www.science.uva.nl/research/sne/ndl#"
  xmlns:capability="http://www.science.uva.nl/research/sne/ndl/capability#"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:dcterms="http://purl.org/dc/terms/"
  xmlns:domain="http://www.science.uva.nl/research/sne/ndl/domain#"
  xmlns:layer="http://www.science.uva.nl/research/sne/ndl/layer#"
  xmlns:physical="http://www.science.uva.nl/research/sne/ndl/physical#"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:vs="http://www.w3.org/2003/06/sw-vocab-status/ns#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
  xmlns:wdm="http://www.science.uva.nl/research/sne/ndl/wdm#"
>

```

```

<rdf:Description rdf:about="http://www.science.uva.nl/research/sne/ndl/wdm#">
  <rdfs:isDefinedBy rdf:resource="http://www.science.uva.nl/research/sne/schema/wdm.rdf"/>
<!-- the schema -->
  <vs:userdocs rdf:resource="http://www.science.uva.nl/research/sne/ndl/?c=20-Technology-
Schemas"/> <!-- human readable info -->
</rdf:Description>

<rdf:Description rdf:about="">
  <!-- meta data on this document itself -->
  <rdfs:label xml:lang="en">Configuration of Speculaas</rdfs:label>
  <dc:title xml:lang="en">Configuration of Speculaas</dc:title>
  <dc:description xml:lang="en">Configuration of the Speculaas switch at Netherlight. This
file is semi-dynamically generated by a cron job that logs in the devices and retrieves all
information. You should expect this data to be stale for about 5 minutes. If you really need real-
time data, then don't use NDL, but another mechanism (e.g. a routing protocol).</dc:description>
  <dc:publisher xml:lang="en">glimmerglassconfig.py script on
ndl.uva.netherlight.nl</dc:publisher>
  <dcterms:issued>2007-01-31</dcterms:issued>
  <dcterms:modified>2007-12-12T15:17:11+0100</dcterms:modified>
</rdf:Description>

<ndl:Device rdf:about="http://speculaas.uva.netherlight.nl#Speculaas">
  <rdfs:label>Speculaas</rdfs:label>
  <dc:description xml:lang="en">Speculaas Glimmerglass OXC</dc:description>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf01"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf02"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf03"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf04"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf05"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf06"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf07"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf08"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf09"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf10"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf11"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf12"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf13"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf14"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf15"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf16"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf17"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf18"/>
  <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf19"/>
  <capability:hasSwitchMatrix>
    <capability:SwitchMatrix
rdf:about="http://speculaas.uva.netherlight.nl#FiberSwitchMatrix">
      <capability:hasSwitchingCapability
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement" />
      <capability:hasSwappingCapability
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement" />
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf01"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf02"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf03"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf04"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf05"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf06"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf07"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf08"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf09"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf10"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf11"/>
      <ndl:hasInterface rdf:resource="http://speculaas.uva.netherlight.nl#intf12"/>
    </capability:SwitchMatrix>
  </capability:hasSwitchMatrix>
</ndl:Device>

<ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf01">
  <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement" />
  <!-- static FiberInterface -->
  <rdfs:label>1</rdfs:label>
  <dc:description xml:lang="en">Rembrandt0 (10GE)</dc:description>
  <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
3.29</wdm:ingressPowerLevel>
  <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
53.03</wdm:egressPowerLevel>
</ndl:Interface>

<ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf02">

```

```

    <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement"/>
    <!-- static FiberInterface -->
    <rdfs:label>2</rdfs:label>
    <dc:description xml:lang="en">Rembrandt1 (10GE)</dc:description>
    <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
3.76</wdm:ingressPowerLevel>
    <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
52.22</wdm:egressPowerLevel>
    </ndl:Interface>

    <ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf03">
    <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement"/>
    <!-- static FiberInterface -->
    <rdfs:label>3</rdfs:label>
    <dc:description xml:lang="en">Rembrandt2 (10GE)</dc:description>
    <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
2.52</wdm:ingressPowerLevel>
    <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
52.60</wdm:egressPowerLevel>
    </ndl:Interface>

    <ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf04">
    <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement"/>
    <!-- static FiberInterface -->
    <rdfs:label>4</rdfs:label>
    <dc:description xml:lang="en">Rembrandt3 (10GE)</dc:description>
    <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
3.77</wdm:ingressPowerLevel>
    <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
52.37</wdm:egressPowerLevel>
    </ndl:Interface>

    <ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf05">
    <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement"/>
    <!-- static FiberInterface -->
    <rdfs:label>5</rdfs:label>
    <dc:description xml:lang="en">Rembrandt4 (10GE)</dc:description>
    <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
2.90</wdm:ingressPowerLevel>
    <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
53.03</wdm:egressPowerLevel>
    <ndl:switchedTo rdf:resource="http://speculaas.uva.netherlight.nl#intf46"/>
    </ndl:Interface>

    <ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf06">
    <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement"/>
    <!-- static FiberInterface -->
    <rdfs:label>6</rdfs:label>
    <dc:description xml:lang="en">Rembrandt5 (10GE)</dc:description>
    <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
3.67</wdm:ingressPowerLevel>
    <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
53.51</wdm:egressPowerLevel>
    </ndl:Interface>

    <ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf09">
    <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement"/>
    <!-- static FiberInterface -->
    <rdfs:label>9</rdfs:label>
    <dc:description xml:lang="en">Rembrandt8 (10GE)</dc:description>
    <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
3.80</wdm:ingressPowerLevel>
    <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
53.84</wdm:egressPowerLevel>
    </ndl:Interface>

    <ndl:Interface rdf:about="http://speculaas.uva.netherlight.nl#intf10">
    <rdf:type
rdf:resource="http://www.science.uva.nl/research/sne/ndl/wdm#FiberNetworkElement"/>
    <!-- static FiberInterface -->
    <rdfs:label>10</rdfs:label>
    <dc:description xml:lang="en">Houdini 10/1 (ex BC 6a.4)</dc:description>
    <wdm:ingressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
4.18</wdm:ingressPowerLevel>

```

```

    <wdm:egressPowerLevel rdf:datatype="http://www.w3.org/2001/XMLSchema#float">-
52.01</wdm:egressPowerLevel>
    </ndl:Interface>

</rdf:RDF>

```

### 3) OSCARS topology description format

```

<?xml version="1.0" encoding="UTF-8"?>
<staticPathDatabase xmlns="http://hopi.internet2.edu/DRAGON/TERCE/RCE/STATICPATHS" id="blue-paths">

<!-- INTRADOMAIN PATHS -->

<!-- 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>

<!-- blue-es2 to blue-es1 -->
<staticPathEntry id="blue-es2-blue-es1">
  <srcEndpoint>urn:ogf:network:domain=blue.pod.lan:node=vlsr3:port=3:link=11.2.5.1</srcEndpoint>
  <destEndpoint>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2</destEndpoint>
  <path id="blue-es2-blue-es1">
    <hop id="1">

<linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr3:port=3:link=11.2.5.1</linkIdRef>
    </hop>
    <hop id="2">

<linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr3:port=5:link=11.2.3.2</linkIdRef>
    </hop>
    <hop id="3">

<linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=5:link=11.2.3.1</linkIdRef>
    </hop>
    <hop id="4">

<linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2</linkIdRef>
    </hop>
  </path>
  <availableVtags></availableVtags> <!-- deprecated: leave blank -->
</staticPathEntry>

<!-- the local portion of the path from blue-es1 to red-es1 -->
<staticPathEntry id="blue-es1-red-es1.local">
  <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=vlsr1:port=6:link=11.1.11.2</destEndpoint>
  <path id="blue-es1-red-es1.local">
    <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=6:link=11.1.11.2</linkIdRef>

```

```

    </hop>
  </path>
  <availableVtags></availableVtags> <!-- deprecated: leave blank -->
</staticPathEntry>

<!-- the local portion of the path from red-es1 to blue-es1 -->
<staticPathEntry id="red-es1-blue-es1.local">
  <srcEndpoint>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=6:link=11.1.11.2/srcEndpoint>
  <destEndpoint>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2</destEndpoint>
  <path id="red-es1-blue-es1.local">
    <hop id="1">

<linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=6:link=11.1.11.2</linkIdRef>
    </hop>
    <hop id="2">

<linkIdRef>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2</linkIdRef>
    </hop>
  </path>
  <availableVtags></availableVtags> <!-- deprecated: leave blank -->
</staticPathEntry>

<!-- INTERDOMAIN PATHS -->
<!-- full interdomain path from blue-es1 to red-es1 -->
<staticPathEntry id="blue-es1-red-es1">
  <srcEndpoint>urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2</srcEndpoint>
  <destEndpoint>urn:ogf:network:domain=red.pod.lan:node=vlsr3:port=4:link=11.1.4.2</destEndpoint>
  <path id="blue-es1-red-es1">
    <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=6:link=11.1.11.2</linkIdRef>
    </hop>
    <hop id="3">

<linkIdRef>urn:ogf:network:domain=red.pod.lan:node=vlsr3:port=6:link=11.1.11.1</linkIdRef>
    </hop>
    <hop id="4">
      <linkIdRef>urn:ogf:network:domain=red.pod.lan:node=vlsr3:port=4:link=11.1.4.2</linkIdRef>
    </hop>
  </path>
  <availableVtags></availableVtags> <!-- deprecated: leave blank -->
</staticPathEntry>
</staticPathDatabase>

```

## Interdomain topology

```

<?xml version="1.0" encoding="UTF-8"?>
<topology
xmlns="http://ogf.ogf/schema/network/topology/ctrlPlane/20071023/"
id="blue-topology">

<idcId>https://idc.blue.pod.lan:8443/axis2/services/OSCARS</idcId>

<domain id="urn:ogf:network:domain=blue.pod.lan">

  <!-- BLUE VLSR1 -->

  <node id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1">
    <address>192.168.2.4</address>

    <!-- intradomain link to blue-es1 -->
    <port id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3">
      <capacity>1000000000</capacity>
      <maximumReservableCapacity>1000000000</maximumReservableCapacity>
      <minimumReservableCapacity>1000000000</minimumReservableCapacity>
      <granularity>100000000</granularity>

      <link id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=3:link=11.2.1.2">
        <remoteLinkId>urn:ogf:network:domain=:node=:port=:link=:</remoteLinkId>
        <trafficEngineeringMetric>100</trafficEngineeringMetric>
        <capacity>1000000000</capacity>
        <maximumReservableCapacity>1000000000</maximumReservableCapacity>
        <minimumReservableCapacity>1000000000</minimumReservableCapacity>

```

```

        <granularity>100000000</granularity>
        <SwitchingCapabilityDescriptors>
            <switchingcapType>l2sc</switchingcapType>
            <encodingType>ethernet</encodingType>
            <switchingCapabilitySpecificInfo>
                <interfaceMTU>9000</interfaceMTU>
                <vlanRangeAvailability>100-200</vlanRangeAvailability>
            </switchingCapabilitySpecificInfo>
        </SwitchingCapabilityDescriptors>
    </link>
</port>

    <!-- intradomain link to blue-vlsr2 -->
    <port id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=4">
        <capacity>1000000000</capacity>
        <maximumReservableCapacity>1000000000</maximumReservableCapacity>
        <minimumReservableCapacity>100000000</minimumReservableCapacity>
        <granularity>100000000</granularity>

        <link id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=4:link=11.2.2.1">

<remoteLinkId>urn:ogf:network:domain=blue.pod.lan:node=vlsr2:port=3:link=11.2.2.2</remoteLinkId>
            <trafficEngineeringMetric>100</trafficEngineeringMetric>
            <capacity>1000000000</capacity>
            <maximumReservableCapacity>1000000000</maximumReservableCapacity>
            <minimumReservableCapacity>100000000</minimumReservableCapacity>
            <granularity>100000000</granularity>
            <SwitchingCapabilityDescriptors>
                <switchingcapType>l2sc</switchingcapType>
                <encodingType>ethernet</encodingType>
                <switchingCapabilitySpecificInfo>
                    <interfaceMTU>9000</interfaceMTU>
                    <vlanRangeAvailability>100-200</vlanRangeAvailability>
                </switchingCapabilitySpecificInfo>
            </SwitchingCapabilityDescriptors>
        </link>
    </port>

    <!-- intradomain link to blue-vlsr3 -->
    <port id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=5">
        <capacity>1000000000</capacity>
        <maximumReservableCapacity>1000000000</maximumReservableCapacity>
        <minimumReservableCapacity>100000000</minimumReservableCapacity>
        <granularity>100000000</granularity>

        <link id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=5:link=11.2.3.1">

<remoteLinkId>urn:ogf:network:domain=blue.pod.lan:node=vlsr3:port=5:link=11.2.3.2</remoteLinkId>
            <trafficEngineeringMetric>100</trafficEngineeringMetric>
            <capacity>1000000000</capacity>
            <maximumReservableCapacity>1000000000</maximumReservableCapacity>
            <minimumReservableCapacity>100000000</minimumReservableCapacity>
            <granularity>100000000</granularity>
            <SwitchingCapabilityDescriptors>
                <switchingcapType>l2sc</switchingcapType>
                <encodingType>ethernet</encodingType>
                <switchingCapabilitySpecificInfo>
                    <interfaceMTU>9000</interfaceMTU>
                    <vlanRangeAvailability>100-200</vlanRangeAvailability>
                </switchingCapabilitySpecificInfo>
            </SwitchingCapabilityDescriptors>
        </link>
    </port>

    <!-- interdomain link to red-vlsr3 -->
    <port id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=6">
        <capacity>1000000000</capacity>
        <maximumReservableCapacity>1000000000</maximumReservableCapacity>
        <minimumReservableCapacity>100000000</minimumReservableCapacity>
        <granularity>100000000</granularity>

        <link id="urn:ogf:network:domain=blue.pod.lan:node=vlsr1:port=6:link=11.1.11.2">

<remoteLinkId>urn:ogf:network:domain=red.pod.lan:node=vlsr3:port=6:link=11.1.11.1</remoteLinkId>
            <trafficEngineeringMetric>100</trafficEngineeringMetric>
            <capacity>1000000000</capacity>
            <maximumReservableCapacity>1000000000</maximumReservableCapacity>
            <minimumReservableCapacity>100000000</minimumReservableCapacity>
            <granularity>100000000</granularity>
            <SwitchingCapabilityDescriptors>
                <switchingcapType>l2sc</switchingcapType>

```

```

        <encodingType>ethernet</encodingType>
        <switchingCapabilitySpecficInfo>
            <interfaceMTU>9000</interfaceMTU>
            <vlanRangeAvailability>100-200</vlanRangeAvailability>
        </switchingCapabilitySpecficInfo>
    </SwitchingCapabilityDescriptors>
</link>
</port>
</node>
</topology>

```

## Intradomain topology example

```

<?xml version="1.0" encoding="UTF-8"?>
<topology
xmlns="http://ogf.ogf/schema/network/topology/ctrlPlane/20071023/"
id="uva-topology">

<idcId>https://idc.blue.pod.lan:8443/axis2/services/OSCARs</idcId>

<domain id="urn:ogf:network:domain=uva.nl">

<node id="urn:ogf:network:domain=uva.nl:node=uva-nodel">
    <address>127.0.0.1</address>

    <port id="urn:ogf:network:domain=uva.nl:node=uva-nodel:port=pizza1">
        <capacity>1000000000</capacity>
        <maximumReservableCapacity>1000000000</maximumReservableCapacity>
        <minimumReservableCapacity>1000000000</minimumReservableCapacity>
        <granularity>100000000</granularity>

        <link id="urn:ogf:network:domain=uva.nl:node=uva-nodel:port=pizza1:link=pizza1">
            <remoteLinkId>urn:ogf:network:domain=*:node=*:port=*:link=*</remoteLinkId>
            <trafficEngineeringMetric>100</trafficEngineeringMetric>
            <capacity>1000000000</capacity>
            <maximumReservableCapacity>1000000000</maximumReservableCapacity>
            <minimumReservableCapacity>1000000000</minimumReservableCapacity>
            <granularity>100000000</granularity>
            <SwitchingCapabilityDescriptors>
                <switchingcapType>l2sc</switchingcapType>
                <encodingType>ethernet</encodingType>
                <switchingCapabilitySpecficInfo>
                    <interfaceMTU>9000</interfaceMTU>
                    <vlanRangeAvailability>0,3000-4000</vlanRangeAvailability>
                </switchingCapabilitySpecficInfo>
            </SwitchingCapabilityDescriptors>
        </link>
    </port>

    <port id="urn:ogf:network:domain=uva.nl:node=uva-nodel:port=nortel">
        <capacity>1000000000</capacity>
        <maximumReservableCapacity>1000000000</maximumReservableCapacity>
        <minimumReservableCapacity>1000000000</minimumReservableCapacity>
        <granularity>100000000</granularity>

        <link id="urn:ogf:network:domain=uva.nl:node=uva-nodel:port=nortel:link=nortel">
            <remoteLinkId>urn:ogf:network:domain=*:node=*:port=*:link=*</remoteLinkId>
            <trafficEngineeringMetric>100</trafficEngineeringMetric>
            <capacity>1000000000</capacity>
            <maximumReservableCapacity>1000000000</maximumReservableCapacity>
            <minimumReservableCapacity>1000000000</minimumReservableCapacity>
            <granularity>100000000</granularity>
            <SwitchingCapabilityDescriptors>
                <switchingcapType>l2sc</switchingcapType>
                <encodingType>ethernet</encodingType>
                <switchingCapabilitySpecficInfo>
                    <interfaceMTU>9000</interfaceMTU>
                    <vlanRangeAvailability>0,3000-4000</vlanRangeAvailability>
                </switchingCapabilitySpecficInfo>
            </SwitchingCapabilityDescriptors>
        </link>
    </port>
</node>
</domain>
</topology>

```



## Appendix C - XACML Identifiers (as defined in XACML2.0 specification [XACML2.0])

Note: This excerpt from the XACML2.0 specification is provided for developers assistance.

XACML specification defines a number of attribute identifiers for common use in the "urn:oasis:names:tc:xacml:" namespace. The use of these identifiers in cases where it is possible will ensure better interoperability.

All other attribute identifiers which in many cases can be application specific are expected to use their own namespaces.

[Appendix B. XACML identifiers (normative)]

[B.1. XACML namespaces]

urn:oasis:names:tc:xacml:2.0:policy:schema:os

urn:oasis:names:tc:xacml:2.0:context:schema:os

[B.2. Access subject categories]

urn:oasis:names:tc:xacml:1.0:subject-category:access-subject

urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject

urn:oasis:names:tc:xacml:1.0:subject-category:intermediary-subject

urn:oasis:names:tc:xacml:1.0:subject-category:codebase

urn:oasis:names:tc:xacml:1.0:subject-category:requesting-machine

[B.3. Data-types]

These identifiers indicate data-types that are defined in the XACML specification Section A.2.

urn:oasis:names:tc:xacml:1.0:data-type:x500Name.

urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name

urn:oasis:names:tc:xacml:2.0:data-type:ipAddress

urn:oasis:names:tc:xacml:2.0:data-type:dnsName

The following data-type identifiers are defined by XML Schema.

<http://www.w3.org/2001/XMLSchema#string>

<http://www.w3.org/2001/XMLSchema#boolean>

<http://www.w3.org/2001/XMLSchema#integer>

<http://www.w3.org/2001/XMLSchema#double>  
<http://www.w3.org/2001/XMLSchema#time>  
<http://www.w3.org/2001/XMLSchema#date>  
<http://www.w3.org/2001/XMLSchema#dateTime>  
<http://www.w3.org/2001/XMLSchema#anyURI>  
<http://www.w3.org/2001/XMLSchema#hexBinary>  
<http://www.w3.org/2001/XMLSchema#base64Binary>

The following data-type identifiers correspond to the `dayTimeDuration` and `yearMonthDuration` data-types defined in [XF Sections 8.2.2 and 8.2.1, respectively].

<http://www.w3.org/TR/2002/WD-xquery-operators-20020816#dayTimeDuration>  
<http://www.w3.org/TR/2002/WD-xquery-operators-20020816#yearMonthDuration>

#### [B.4. Subject attributes]

These identifiers indicate attributes of a subject. When used, they SHALL appear within a `<Subject>` element of the request context. They SHALL be accessed by means of a `<SubjectAttributeDesignator>` element, or an `<AttributeSelector>` element that points into a `<Subject>` element of the request context.

At most one of each of these attributes is associated with each subject. Each attribute associated with authentication included within a single `<Subject>` element relates to the same authentication event. This identifier indicates the name of the subject. The default format is “`http://www.w3.org/2001/XMLSchema#string`”. To indicate other formats, use the `DataType` attributes listed in B.3

`urn:oasis:names:tc:xacml:1.0:subject:subject-id`

This identifier indicates the subject's ID e.g. in a form of string, RFC822, or LDAP X.511 format

`urn:oasis:names:tc:xacml:1.0:subject:category`

This identifier indicates the subject category. “access-subject” is the default value.

`urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier`

This identifier indicates the security domain of the subject. It identifies the administrator and policy that manages the name-space in which the subject id is administered.

`urn:oasis:names:tc:xacml:1.0:subject:key-info`

This identifier indicates a public key used to confirm the subject's identity.

`urn:oasis:names:tc:xacml:1.0:subject:authentication-time`

This identifier indicates the time at which the subject was authenticated.

`urn:oasis:names:tc:xacml:1.0:subject:authn-locality:authentication-method`

This identifier indicates the method used to authenticate the subject.

urn:oasis:names:tc:xacml:1.0:subject:request-time

This identifier indicates the time at which the subject initiated the access request, according to the PEP.

urn:oasis:names:tc:xacml:1.0:subject:session-start-time

This identifier indicates the time at which the subject's current session began, according to the PEP.

The following identifiers indicate the location where authentication credentials were activated. They are intended to support the corresponding entities from the SAML authentication statement.

urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-address

This identifier indicates that the location is expressed as an IP address.

The corresponding attribute SHALL be of data-type "<http://www.w3.org/2001/XMLSchema#string>".

urn:oasis:names:tc:xacml:1.0:subject:authn-locality:dns-name

This identifier indicates that the location is expressed as a DNS name.

The corresponding attribute SHALL be of data-type "<http://www.w3.org/2001/XMLSchema#string>".

Where a suitable attribute is already defined in LDAP [LDAP-1, LDAP-2], the XACML identifier SHALL be formed by adding the attribute name to the URI of the LDAP specification. For example, the attribute name for the userPassword defined in the RFC 2256 SHALL be:

<http://www.ietf.org/rfc/rfc2256.txt#userPassword>

#### [B.6. Resource attributes]

urn:oasis:names:tc:xacml:1.0:resource:resource-id

These identifiers indicate attributes of the resource. The corresponding attributes MAY appear in the <Resource> element of the request context and be accessed by means of a <ResourceAttributeDesignator> element, or by an <AttributeSelector> element that points into the <Resource> element of the request context. This attribute identifies the resource to which access is requested. If an <xacml-context:ResourceContent> element is provided, then the resource to which access is requested SHALL be all or a portion of the resource supplied in the <xacml-context:ResourceContent> element.

urn:oasis:names:tc:xacml:2.0:resource:target-namespace

This attribute identifies the namespace of the top element of the contents of the <xacml-context:ResourceContent> element. In the case where the resource content is supplied in the request context and the resource namespace is defined in the resource, the PDP SHALL confirm that the namespace defined by this attribute is the same as that defined in the resource. The type of the corresponding attribute SHALL be "<http://www.w3.org/2001/XMLSchema#anyURI>".

#### [B.7. Action attributes]

These identifiers indicate attributes of the action being requested. When used, they SHALL appear within the <Action> element of the request context. They SHALL be accessed by means of an <ActionAttributeDesignator> element, or an <AttributeSelector> element that points into the <Action> element of the request context.

urn:oasis:names:tc:xacml:1.0:action:action-id

This attribute identifies the action for which access is requested.

Where the action is implicit, the value of the action-id attribute SHALL be

urn:oasis:names:tc:xacml:1.0:action:implied-action

#### [B.8. Environment attributes]

These identifiers indicate attributes of the environment within which the decision request is to be evaluated. When used in the decision request, they SHALL appear in the <Environment> element of the request context. They SHALL be accessed by means of an <EnvironmentAttributeDesignator> element, or an <AttributeSelector> element that points into the <Environment> element of the request context.

urn:oasis:names:tc:xacml:1.0:environment:current-time

urn:oasis:names:tc:xacml:1.0:environment:current-date

urn:oasis:names:tc:xacml:1.0:environment:current-dateTime

#### [B.9. Status codes]

The following status code values are defined.

urn:oasis:names:tc:xacml:1.0:status:ok

urn:oasis:names:tc:xacml:1.0:status:missing-attribute

urn:oasis:names:tc:xacml:1.0:status:syntax-error

urn:oasis:names:tc:xacml:1.0:status:processing-error

#### [B.10. Combining algorithms]

The deny-overrides rule-combining algorithm has the following value for the ruleCombiningAlgId attribute:

urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides

urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides

urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides

urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides

urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable

urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable

urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:only-one-applicable

urn:oasis:names:tc:xacml:1.1:rule-combining-algorithm:ordered-deny-overrides

urn:oasis:names:tc:xacml:1.1:policy-combining-algorithm:ordered-deny-overrides

urn:oasis:names:tc:xacml:1.1:rule-combining-algorithm:ordered-permit-overrides

urn:oasis:names:tc:xacml:1.1:policy-combining-algorithm:ordered-permit-overrides

## Appendix D - XACML-Grid profile Identifiers [XACML-Grid]

Note: This excerpt from the XACML-Grid profile specification is provided for developers assistance.

### 1. List of Attribute and Obligation IDs introduced by the XACML-Grid profile

#### Namespace used in XACML-Grid profile

*http://authz-interop.org/xacml*

#### Subject Context

*http://authz-interop.org/xacml/subject/subject-x509-id*

*http://authz-interop.org/xacml/subject/subject-condor-canonical-name-id*

*http://authz-interop.org/xacml/subject/subject-x509-issuer*

*http://authz-interop.org/xacml/subject/vo*

*http://authz-interop.org/xacml/subject/voms-signing-subject*

*http://authz-interop.org/xacml/subject/voms-signing-issuer*

*http://authz-interop.org/xacml/subject/voms-fqan*

*http://authz-interop.org/xacml/subject/voms-primary-fqan*

#### Optional Attributes:

*http://authz-interop.org/xacml/subject/certificate-serial-number*

*http://authz-interop.org/xacml/subject/ca-serial-number*

*http://authz-interop.org/xacml/subject/voms-dns-port*

*http://authz-interop.org/xacml/subject/ca-policy-oid*

*http://authz-interop.org/xacml/subject/cert-chain*

#### Action Context

Enumeration of possible values for *urn:oasis:names:tc:xacml:1.0:action:action-id* :

*http://authz-interop.org/xacml/action/action-type/queue*

*http://authz-interop.org/xacml/action/action-type/execute-now*

*http://authz-interop.org/xacml/action/action-type/access*

*http://authz-interop.org/xacml/action/rsl-string*

#### Resource Context

Enumeration of possible values for *urn:oasis:names:tc:xacml:1.0:resource:resource-id* :

*http://authz-interop.org/xacml/resource/resource-type/ce*

*http://authz-interop.org/xacml/resource/resource-type/se*

<http://authz-interop.org/xacml/resource/resource-type/wn>

<http://authz-interop.org/xacml/resource/dns-host-name>

<http://authz-interop.org/xacml/resource/resource-x509-id>

<http://authz-interop.org/xacml/resource/resource-x509-issuer>

### **Environment Context**

<http://authz-interop.org/xacml/environment/pilot-job/pep-oblig-supported>

<http://authz-interop.org/xacml/environment/pilot-job/subject-x509-id>

<http://authz-interop.org/xacml/environment/pilot-job/subject-condor-canonical-name-id>

<http://authz-interop.org/xacml/environment/pilot-job/subject-x509-issuer>

<http://authz-interop.org/xacml/environment/pilot-job/vo>

<http://authz-interop.org/xacml/environment/pilot-job/voms-signing-subject>

<http://authz-interop.org/xacml/environment/pilot-job/voms-signing-issuer>

<http://authz-interop.org/xacml/environment/pilot-job/voms-fqan>

<http://authz-interop.org/xacml/environment/pilot-job/voms-primary-fqan>

### **Obligation Context and Attributes**

<http://authz-interop.org/xacml/obligation/uidgid>

<http://authz-interop.org/xacml/attribute/posix-uid>

<http://authz-interop.org/xacml/attribute/posix-uid>

<http://authz-interop.org/xacml/obligation/secondary-gids>

<http://authz-interop.org/xacml/attribute/posix-gid>

<http://authz-interop.org/xacml/obligation/username>

<http://authz-interop.org/xacml/attribute/username>

<http://authz-interop.org/xacml/obligation/afs-token>

<http://authz-interop.org/xacml/attribute/afs-token>

<http://authz-interop.org/xacml/obligation/root-and-home-paths>

<http://authz-interop.org/xacml/attribute/rootpath>

<http://authz-interop.org/xacml/attribute/homepath>

<http://authz-interop.org/xacml/obligation/storage-access-priority>

<http://authz-interop.org/xacml/attribute/storage-priority>

*<http://authz-interop.org/xacml/obligation/access-permissions>*

*<http://authz-interop.org/xacml/attribute/access-permissions>*

## History of changes

- 1) Draft version 0.2 (future) – will provide first initial set of XACML-NRP policies that use topology and user information
- 2) Draft version 0.1 (July 9, 2008) – Added Implementation suggestions for policy resolution and composing PolicyId.
- 3) Draft version 0.0 (May 27, 2008) – initial version presented for the discussion in Phosphorus WPI, WP2, WP4 mailing lists