PHOSPHORUS

Generic Authorisation Infrastructure for on-demand multi-domain Network Resource Provisioning (GAAA-NRP)

Yuri Demchenko <demch@science.uva.nl>
System and Network Engineering Group
University of Amsterdam

Bandwidth on Demand Workshop, TNC2009
7 June 2009, Malaga, Spain

Outline

- Generic AAA/AuthZ Infrastructure for multi-domain Network Resource Provisioning (GAAA-NRP)
  - Network Resource provisioning workflow
- Using tickets and tokens for access control and signalling in multidomain NRP
  - Provisioning and authorisation sessions
- XACML-NRP policy and attributes profile for multidomain NRP
  - Policy Obligations in NRP
- Pluggable GAAA Toolkit Java library to support multidomain NRP
- Future developments

Optical Network Resource Provisioning (NRP) Model

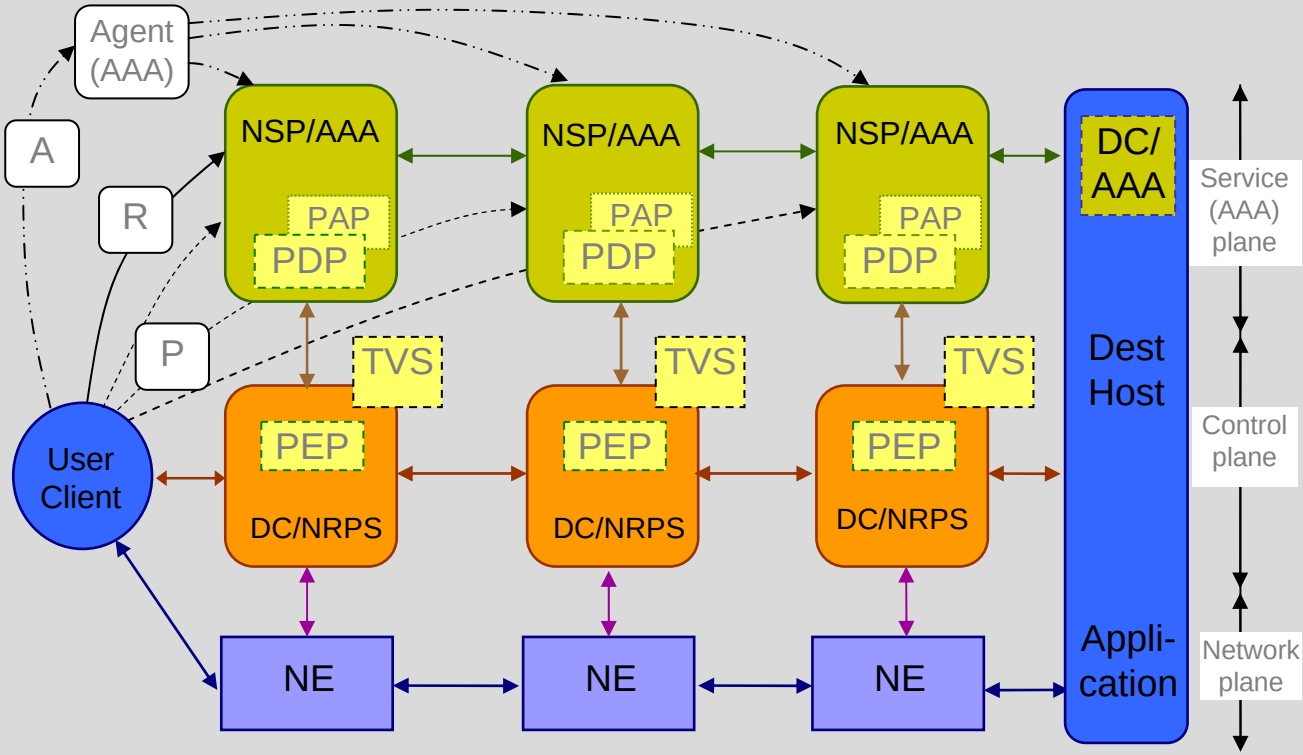
4 major stages/phases in NRP/CRP operation/workflow

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

Rationale

- Specifically oriented on combined Grid-network resource provisioning
- Integrating resource provisioning into the upper layer scientific workflow

Multidomain Network Resource Provisioning (NRP) – Provisioning sequences



Provisioning sequences

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

Token based policy enforcement

GRI – Global Reservation ID

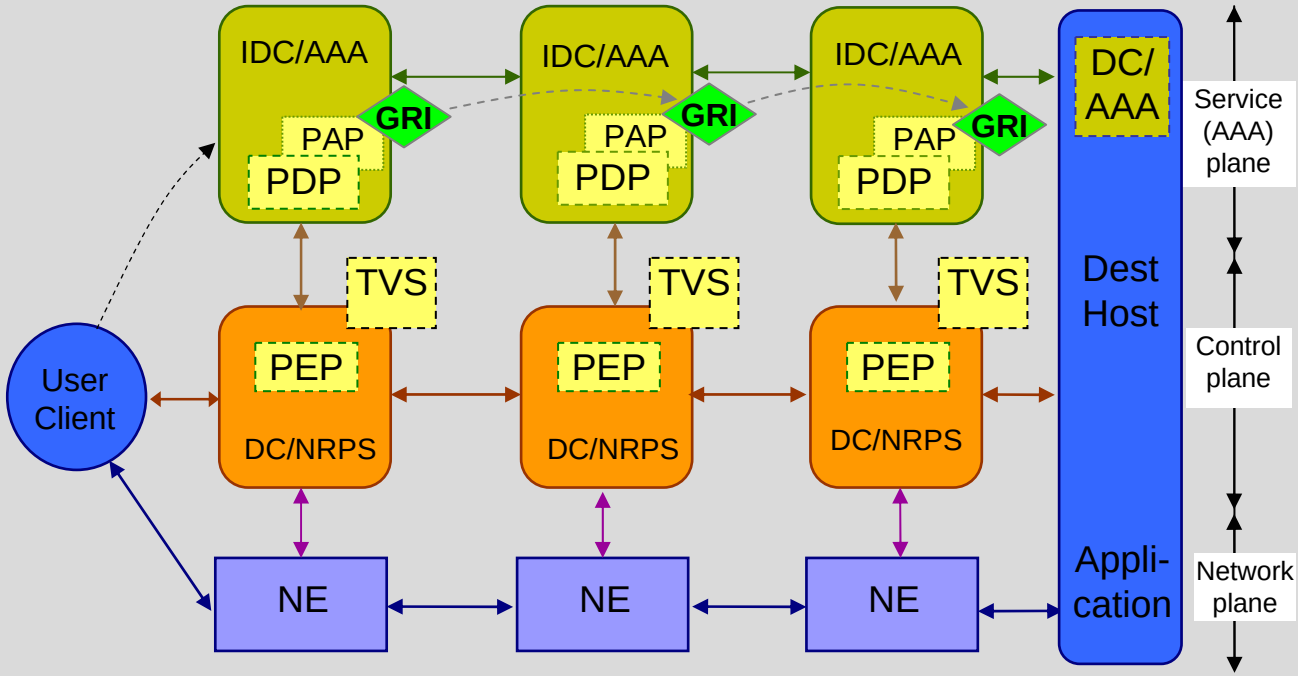
AuthZ tickets for multidomain context mngnt

T - Token

- NRPS – Network Resource Provisioning System
- NSP – Network Service Plain
- DC – Domain Controller
- IDC – Interdomain Controller

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

Multidomain Network Resource Provisioning (NRP) – Stage 1 – Path building and Advance Reservation



Token based signalling and access control

GRI – Global Reservation ID

AzTicket – AuthZ ticket for multidomain context mngnt

AT – Access Token

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

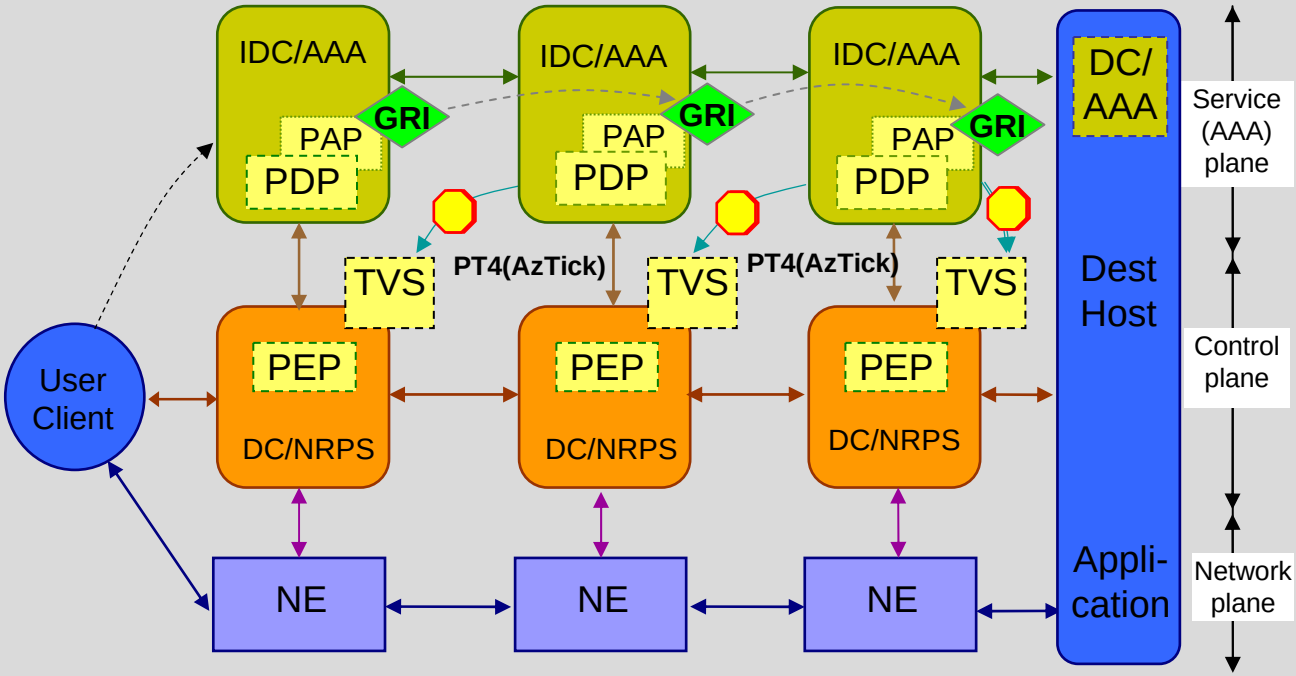
* As container for GRI and AzTicket

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

IDC – Interdomain Controller
DC – Domain Controller
NRPS – Network Resource Provisioning System
NE - Network Element

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

Multidomain Network Resource Provisioning (NRP) – Stage 2 – Deployment (setup and key distribution)



Token based signalling and access control

GRI – Global Reservation ID

AzTicket – AuthZ ticket for multidomain context mngnt

AT – Access Token

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

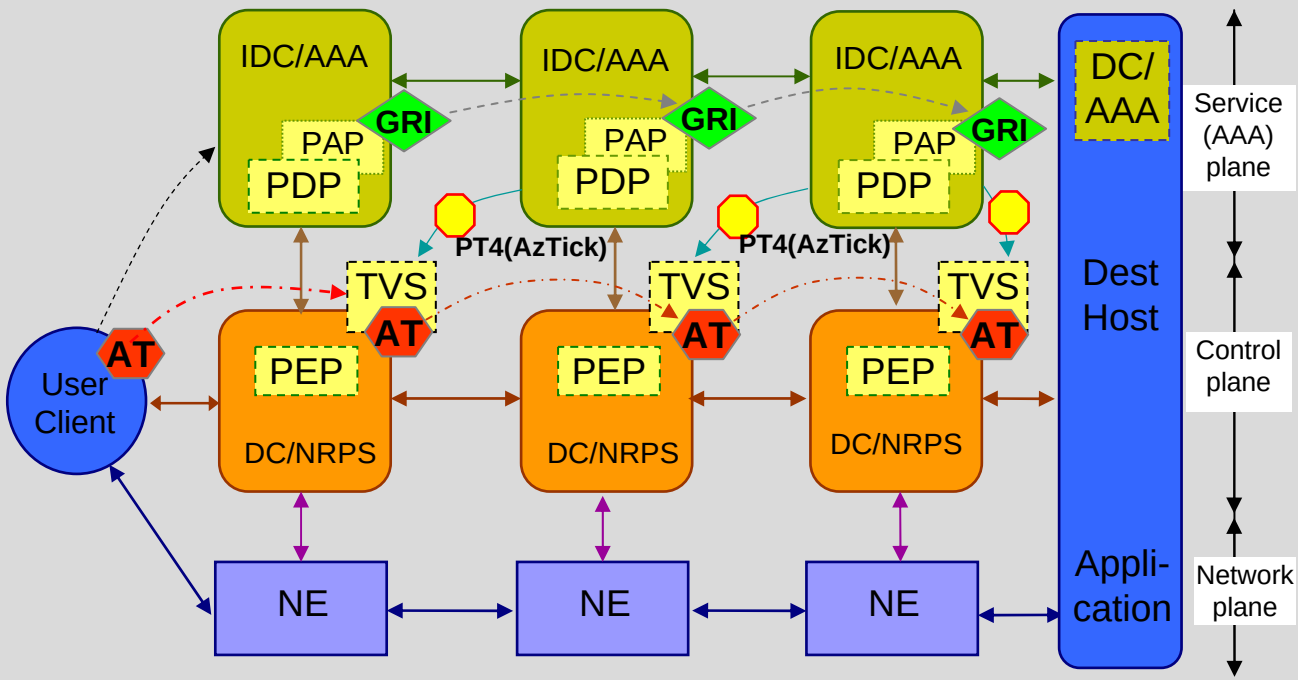
* As container for GRI and AzTicket

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

IDC – Interdomain Controller
DC – Domain Controller
NRPS – Network Resource Provisioning System
NE - Network Element

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

Multidomain Network Resource Provisioning (NRP) – Stage 3 – Access Control (using access tokens)



Token based signalling and access control

GRI – Global Reservation ID

AzTicket – AuthZ ticket for multidomain context mngnt

AT – Access Token

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

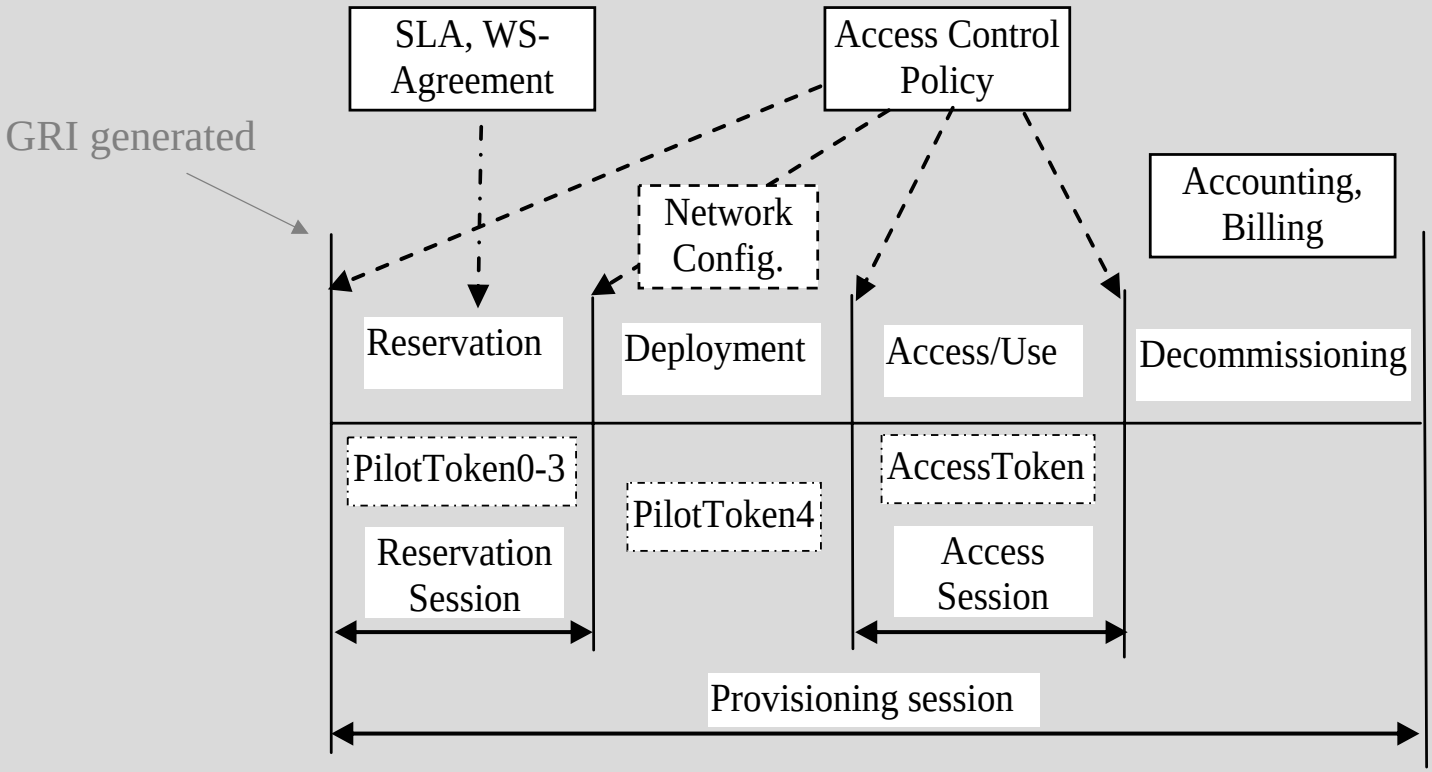
* As container for GRI and AzTicket

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

IDC – Interdomain Controller
DC – Domain Controller
NRPS – Network Resource Provisioning System
NE - Network Element

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

NRP Stages and Authorisation Session Types



- Requires consistent security and session context management
- Global Reservation ID (GRI) is created at the beginning of the provisioning session (Reservation stage) and binds all sessions

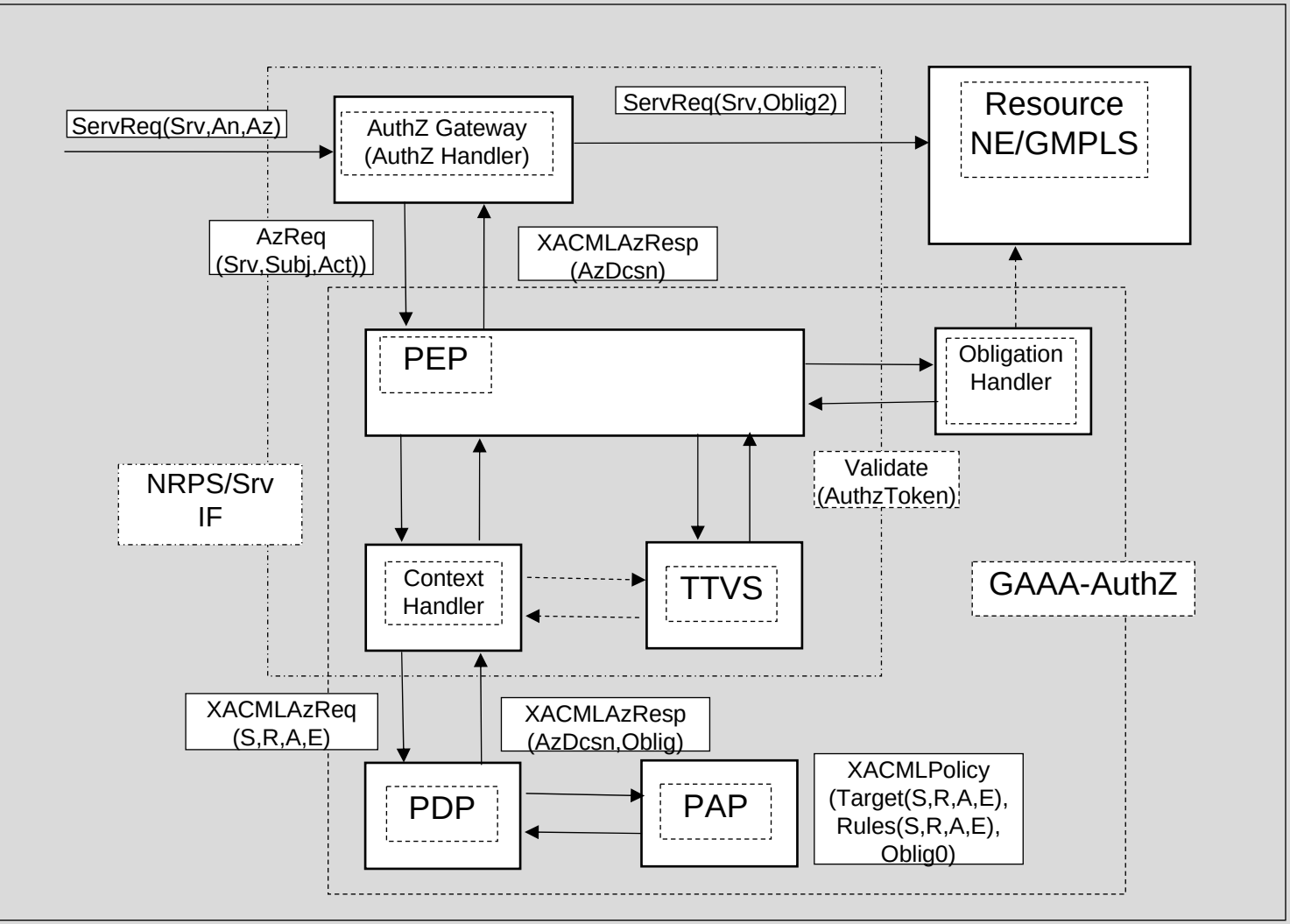
AAA/AuthZ mechanisms and functional components to support multidomain optical NRP

The proposed AAA/security mechanisms and functional components to extend generic AAA AuthZ framework (PEP, PDP, PAP and operational sequences)

- Token Validation Service (TVS) to enable token based policy enforcement
  - Can be applied at all Networking layers (Service, Control and Data planes)
  - *Pilot Token signalling mechanism implemented in the GAAA-TK library*
- AuthZ ticket format for extended AuthZ session management
  - To allow extended AuthZ decision/session context communication between domains
- XACML-NRP attributes and policy profile for NRP
  - Rich functionality of the XACML policy format for complex network and Grid resources
  - *Can add dynamic path/topology information and Policy obligations to policy definition*
- Policy Obligation Handling Reference Model (OHRM)
  - Used for account mapping, quota enforcement, accounting, etc.
- *Identity Based Cryptography (IBC) use for token key distribution in inter-domain network resource provisioning is being investigated*
  - Targeted for the “deployment” stage

- The proposed architecture allows smooth integration with other AuthZ frameworks as currently used and being developed by NREN and Grid community
  - Can provide basic AAA/AuthZ functionality for each network layer DP, CP, SP

GAAA Toolkit Library – Core Components



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

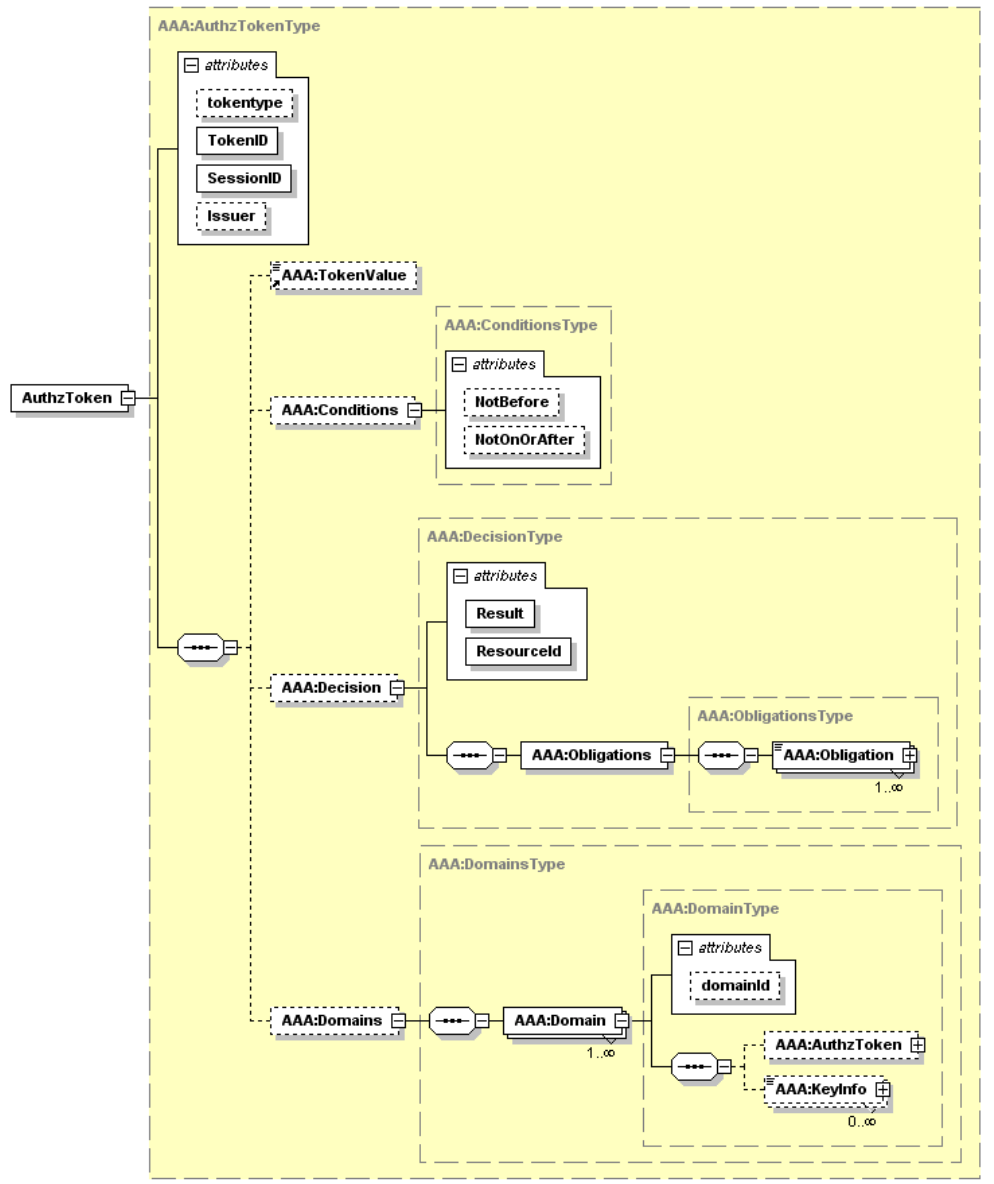
- ContextHandler functionality can be extended to support all communications between PEP-PDP and with other modules

TTVS – Ticket and token validation and handling service

Access Token and Pilot Token Types

- **AType 0** – Simple access token (refers to the reserved resources context)
- **AType 1** – Access token containing Obligations collected from previous domains
- **PType 0** – Container for GRI only
- **PType 1** – Container for communicating the GRI during the reservation stage
  - Contains the mandatory SessionId=GRI attribute and an optional Condition element
- **PType 2** – Origin/requestor authenticating token
  - TokenValue element contains a value that can be used as the authentication value for the token origin
  - TokenValue may be calculated of the (GRI, IssuerId, TokenId) by applying e.g. HMAC function with the requestor's symmetric or private key.
- **PType 3** – Extends Type 2 with the Domains element that allows collecting domains security context information when passing multiple domains during the reservation process
  - Domains' context may include the previous token and the domain's trust anchor or public key
- **PType 4** – Used at the deployment stage and can communicate between domains security context information about all participating in the provisioned lightpath or network infrastructure resources
  - Can be used for programming/setting up a TVS infrastructure for consistent access control tokens processing at the resource access stage

General XML Token Format – Access and Pilot Tokens



- Required functionality to support multidomain provisioning scenarios
  - Allows easy mapping to SAML and XACML related elements
- Allows multiple Attributes format (semantics, namespaces)
- Establish and maintain Trust relations between domains
  - Including Delegation
- Ensure Integrity of the AuthZ decision
  - Keeps AuthN/AuthZ context
  - Allow Obligated Decisions (e.g. XACML)

XML Token Example – Access Token Type 0

```
<AAA:AuthzToken xmlns:AAA="http://www.aaauthreach.org/ns/#AAA"
   Issuer="urn:aaa:gaaapi:token:TVS" type="access-type0"
   SessionId="a9bcf23e70dc0a0cd992bd24e37404c9e1709afb"
   TokenId="d1384ab54bd464d95549ee65cb172eb7">
    <AAA:TokenValue>ebd93120d4337bc3b959b2053e25ca5271a1c17e</AAA:TokenValue>
    <AAA:Conditions NotBefore="2007-08-12T16:00:29.593Z"
        NotOnOrAfter="2007-08-13T16:00:29.593Z"/>
</AAA:AuthzToken>
```

where

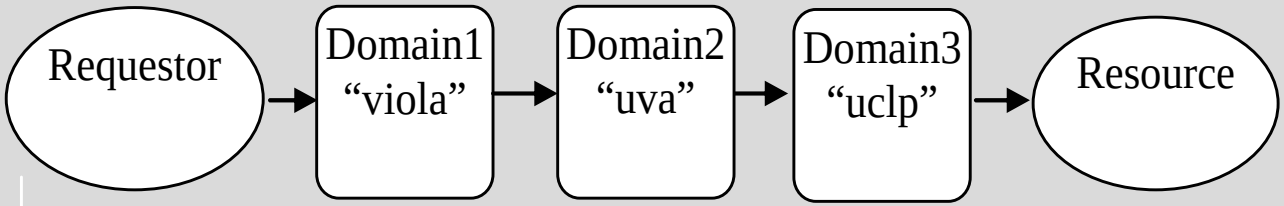
SessionId = GRI (Global Reservation Id)

TokenId – unique identifier (serving for logging and accountability)

TokenValue – generated securely from GRI or AuthzTicket (digital SignatureValue)

- The element <TokenValue> and attributes SessionId and TokenId are mandatory, and the element <Conditions> and attributes Issuer, NotBefore, NotOnOrAfter are optional
- Binary token contains just two values – TokenValue and GRI

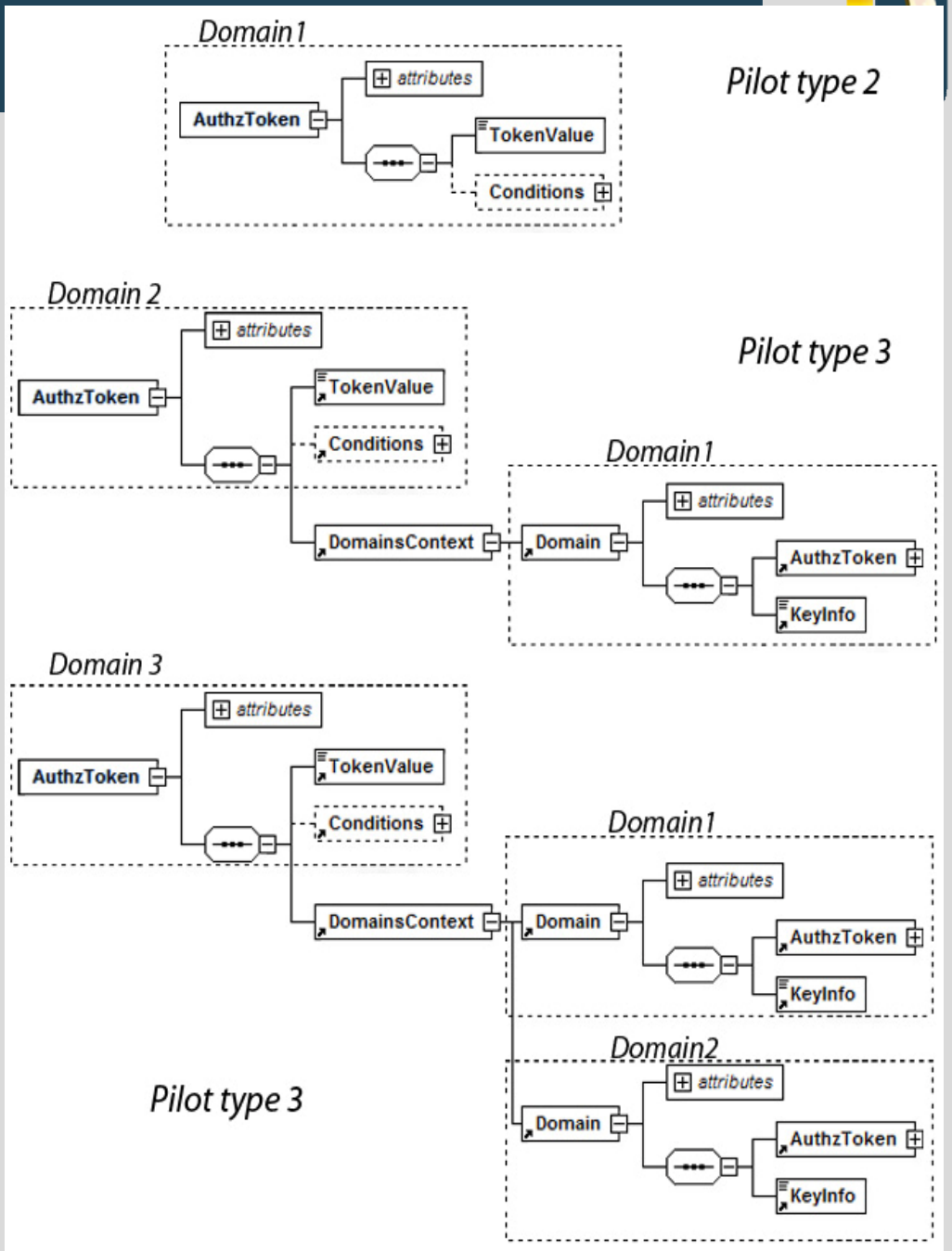
Chaining Pilot Tokens in multidomain signalling



* Pilot Token type 3

```
<AAA:AuthzToken xmlns:AAA="http://www.aaauthreach.org/ns/AAA"
          Issuer=http://testbed.ist-phosphorus.eu/uva/AAA/TVS/tokenpilot
          SessionId="740b241e711ece3b128c97f990c282adcbf476bb"
          TokenId="dc58b505f9690692f7a6312912d0fb4c"  type="pilot-type3">
  <AAA:TokenValue>190a3c1554a500e912ea75a367c822c09eceaa2f </AAA:TokenValue>
  <AAA:Conditions NotBefore="2009-01-30T08:57:40.462Z"  NotOnOrAfter="2009-01-
30T09:21:40.462Z"/>
  <AAA:DomainsContext>
    <AAA:Domain domainId="http://testbed.ist-phosphorus.eu/viola">
      <AAA:AuthzToken Issuer="http://testbed.ist-phosphorus.eu/viola/aaa/TVS/token-pilot«
            SessionId="2515ab7803a86397f3d60c670d199010aa96cb51"
            TokenId="c44a2f5f70346fdc2a2244fecbcdd244">
        <AAA:TokenValue>dee1c29719b9098b361cab4cfcd086700ca2f414
        </AAA:TokenValue>
        <AAA:Conditions NotBefore="2009-01-30T07:57:35.227Z"
                        NotOnOrAfter="2009-01-31T07:57:35.227Z"/>
      </AAA:AuthzToken>
      <AAA:KeyInfo> http://testbed.ist-phosphorus.eu/viola/_public_key_ </AAA:KeyInfo>
    </AAA:Domain>
  </AAA:DomainsContext>
</AAA:AuthzToken>
```

Pilot Tokens Chaining



TVS functionality – Access Control and Signalling

- Basic TVS functionality is checking validity of an access token received from the PEP or AuthZ gateway/service
  - Extended TVS functionality allow token re-building when processing request from the previous domain and relaying to the next domain
    - Special method to Validate&Relay pilot tokens
  - Additionally, TVS may be used for token security context distribution, e.g. token key(s), at the reservation stage or at the stage of the reserved resource deployment
- TVS supports pilot tokens signalling during the reservation stage
  - Can be used for building dynamic security association of the reserved resources
- TVS is implemented as a component and a profile of the GAAA Toolkit GAAAPI package
  - Can be integrated into the target network provisioning systems and applications, in particular OSCARS and DRAGON (result of cooperation with Internet2)
- The current token handling model uses shared secret HMAC-SHA1 algorithm:

```
TokenKey = HMAC(GRI, tb_secret)
TokenValue = HMAC(GRI, DomainId, TokenId, TokenKey)
```

where GRI – global reservation identifier

tb_secret – shared Token Builder secret.

XACML-NRP Profile

- XACML policy and attributes profile for Network Resource Provisioning
  - Defines a number of Subject, Resource, Action, Environment attributes used in the XACML policy definition
  - Defines policy Obligations format and handling model
  - Presented at OGF23 OGSA-AUTHZ Working Group and NML-WG
  - Also a part of the Phosphorus project D4.3.1 deliverable
  - Reference implementation in the GAAA-TK library
  - Recent update (July 2008) - http://staff.science.uva.nl/~demch/projects/aaauthreach/draft-interop-xacml-nrp-profile-012.pdf
  - Considered as an extension of the XACML-Grid profile
    - "An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids" (Joint project by EGEE, OSG, GT). Version 1.0, May 16, 2008 - https://edms.cern.ch/document/929867/1

XACML-NRP Profile – Basic Use Cases for Policy Definition in NRP

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

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

- Suggests using simple delegation scenario intra-domain

Use case 3: “User/Group A is only allowed to invoke method/action X, Y, and Z”

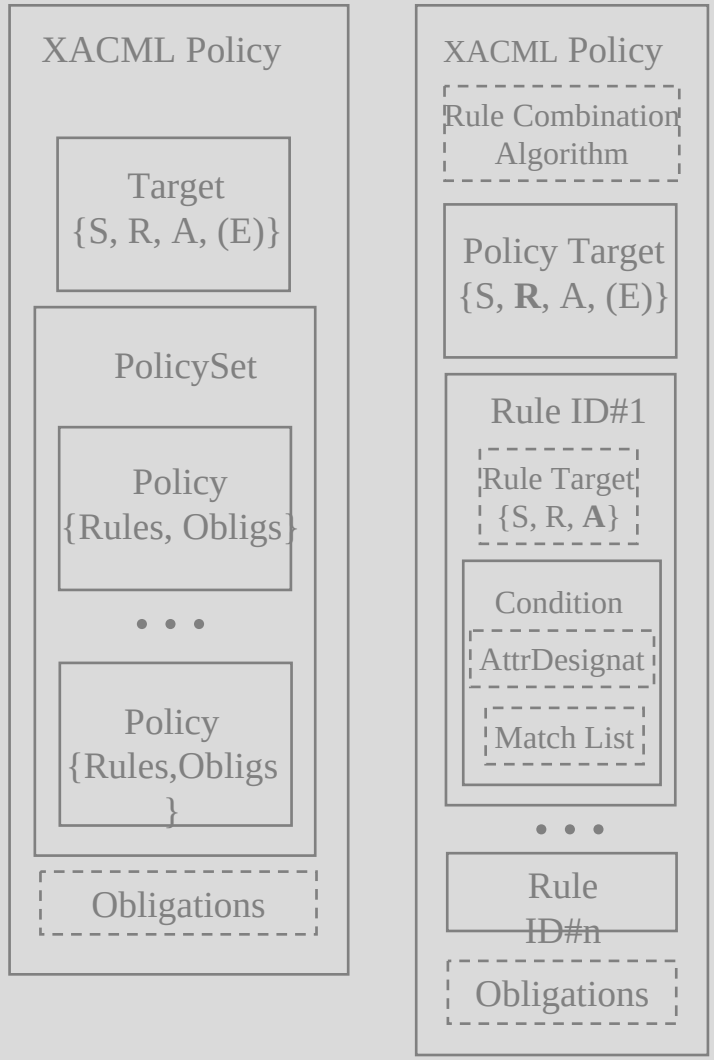
Use case 4: “User/Group A is only allowed to invoke method X,Y, and Z based on session delegation”

- Currently implemented as special PEP methods

- Defined as a result of inter-WP cooperation in Phosphorus
- XACML-NRP profile is implemented as part of the GAAA-TK Java library
  - Intended to be compatible with Globus Toolkit AuthZ framework
  - Supports also XACML-Grid profile developed by OSG and EGEE

XACML Policy format

- XACML standard specifies XACML policy format and XACML request/response messages
- Policy consists of Policy Target and Rules
  - Policy Target is defined for the tuple Subject-Resource-Action (-Environment)
  - Policy Rule consists of Conditions and may contain Obligations
  - Obligation defines actions to be taken by PEP on Policy decision by PDP
- XACML PDP returns all Obligations that match policy decision (defined by attribute “FulfillOn”) from both PolicySet and comprising individual policies
- XACML specification and implementation doesn’t support any functionality related to attributes validation and Obligations handling



XACML Request message - Example

```
<xacml-context:Request xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xacml-
    context="urn:oasis:names:tc:xacml:1.0:context" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:context aaa-msg-xacml-01.xsd">
  <xacml-context:Subject Id="subject"    SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-
    category:access-subject">
    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" admin@gaaa.virtlab.nl ">
      <xacml-context:AttributeValue>WHO740@users.project.organisation.nl</xacml-
    context:AttributeValue> </xacml-context:Attribute>

    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-confdata"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" admin@gaaa.virtlab.nl ">
      <xacml-context:AttributeValue>2SeDFGVHYTY83ZXxEdsweOP8Iok)yGHxVfHom90</xacml-
    context:AttributeValue> </xacml-context:Attribute>

    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-role"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" admin@gaaa.virtlab.nl ">
      <xacml-context:AttributeValue>Analyst</xacml-context:AttributeValue>
    </xacml-context:Attribute> </xacml-context:Subject>

  <xacml-context:Resource>
    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="admin@gaaa.virtlab.nl">
      <xacml-context:AttributeValue>Resource-ID-here</xacml-context:AttributeValue>
    </xacml-context:Attribute>   </xacml-context:Resource>

    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="admin@gaaa.collaboratory.nl">
      <xacml-context:AttributeValue>assign-time</xacml-context:AttributeValue>
    </xacml-context:Attribute>
  </xacml-context:Action> </xacml-context:Request>
```

Subject related Attributes

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

Resource related attributes

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

Describes topology related information

3 topology description formats were reviewed

- Phosphorus NSP/WP1 topology description
- NDL by UvA
- OSCARS (currently used)

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

Action related Attributes and Enumerated values

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

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

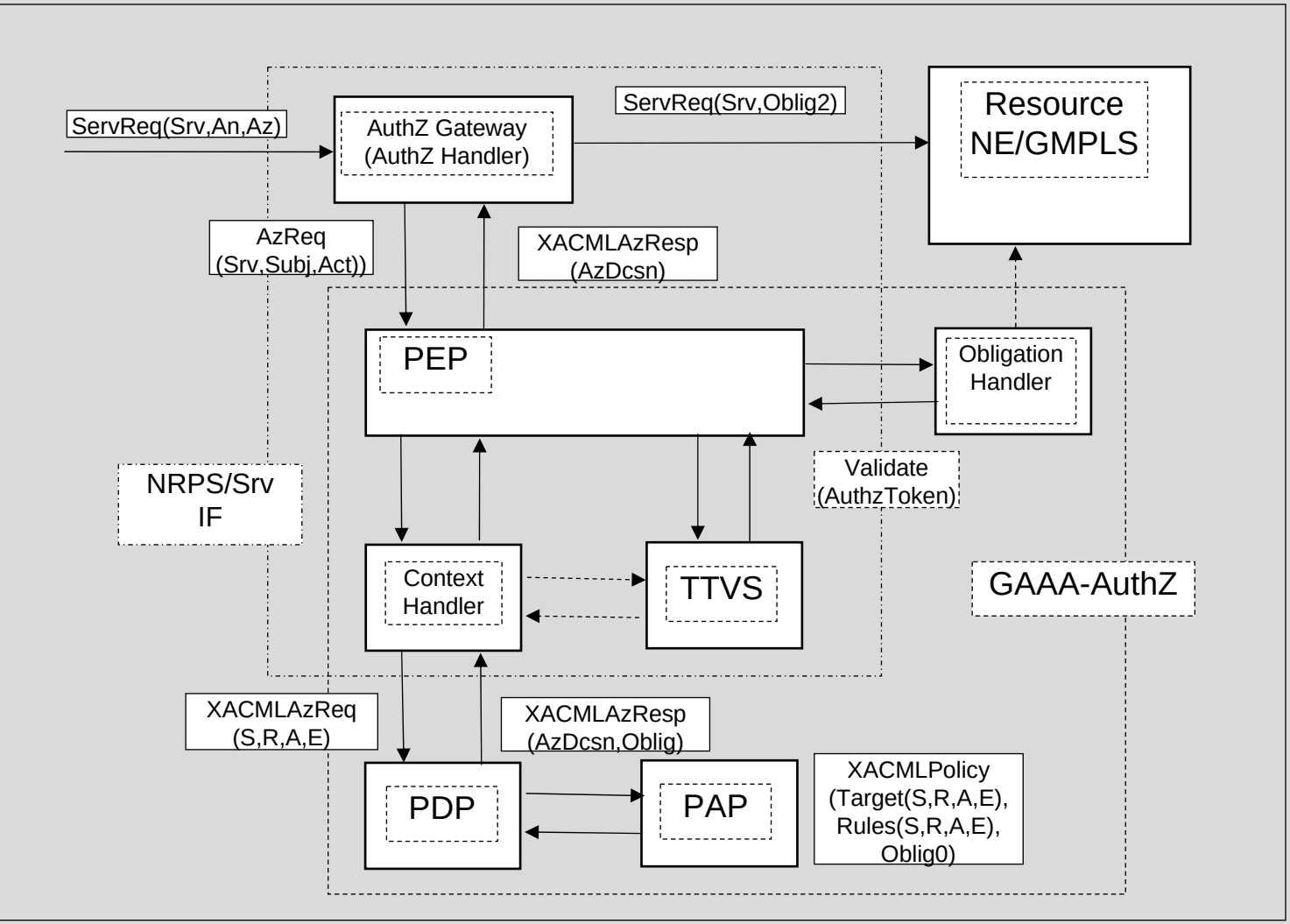
Environment related Attributes

- Last-domain confirmation
- Authorisation context
  - AuthZ session credentials or AuthZ ticket
- Delegation or Obligations from the previous domain
  - User ID or group to which access is delegated
  - Actions which need to be taken when processing request or granting access

Policy Obligations in NRP scenarios

- Policy decision is done at the reservation stage (advance reservation stage often requires policy decision) and actual policy enforcement takes place at the access stage
  - Advance resource reservation (ARR) use cases and Usable/Consumable resources
    - ***Fixed ARR*** that implies strict time/amount constraints
    - ***Deferrable ARR*** that allows some degree of freedom in the time domain with fixed amount (or bandwidth)
    - ***Malleable ARR*** that allows variable duration and amount for the fixed consumption amount
- Policy may contain Obligations and (obligated) policy decision may suggest the following action at later stage
  - Conditional AuthZ decision (e.g. type of service or credentials for multi-domain multi-provider resources)
  - Account mapping
  - Quota assignment
  - Logging and accounting

Implementation - GAAA Toolkit Library



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

- ContextHandler functionality can be extended to support all communications between PEP-PDP and with other modules

TTVS – Ticket and token validation and handling service

GAAA-NRP Implementation – Pluggable GAAA-TK Java library

- XACML-NRP profile is implemented in GAAA-TK Java library
  - Intended to be compatible with Globus Toolkit AuthZ framework
- GAAA-TK library provides all necessary AuthZ mechanisms and service components to support AuthZ sessions context and Obligations handling
  - Supports SAML2.0 profile of XACML – protocol and request/response messages
- Access token and pilot tokens used for access control and signalling
  - Supported by the Token Validation Service (TVS) functionality
  - Can be used transparently at all Networking layers (Service, Control and Data planes)
- AuthZ ticket format for extended AuthZ session management
  - To allow extended AuthZ decision/security context communication between domains
- Allows integration with other AuthZ frameworks (Grid and network middleware)
  - Supports Unicore6 Explicit Trust Delegation SAML Assertions
- Integrated into the Phosphorus project Network Service Plane (NSP) test-bed and uses simple XACML policy model
  - Part of the Phosphorus project deliverable D.4.3.1 - "GAAA toolkit pluggable components and XACML policy profile for ONRP“

Core PEP Methods

Method #1 – base method: receives a set of (Subject, Resource, Action) attributes and return boolean policy decision

`boolean authorizeAction (HashMap resmap, HashMap actmap, HashMap subjmap)`

Provides Subject attributes validation

Security or session context can be supplied as “subject-context” attribute

Method #2 - simple version of method #1

`boolean authorizeAction (String resourceURI, String actions, HashMap subjmap)`

Method #3 - simple version of method #1

`boolean authorizeAction (String resourceId, String actions, String subjectId, String subjconfdata, String roles, String subjctx)`

Method #4 – returns either AuthZ ticket/token or string “Deny”

`String authorizeAction (String authzTicketToken, HashMap resmap, HashMap actmap, HashMap subjmap)`

Can generate initial AuthZ ticket or token if “**`authzTicketToken`**” variable is NULL

Method #5 - simple version on method #4

`String authorizeAction String authorizeAction (String authzTicketToken, String sessionId, String resourceId, String action)`

Can be used for repetitive actions in the same AuthZ session

SessionId is “GRI”

Method #6 - simple version on method #4

`String authorizeAction String authorizeAction (String authzTicketToken, String sessionId, String resourceId, String actions, HashMap subjmap)`

Extended PEP Methods Supporting Token-based Access Control and Signalling with Simple Delegation Functionality

Method #7 - simple intra-domain delegation

```
boolean authorizeActionSession (String authzToken, String griReq,
  int delegtype, HashMap resmap, HashMap actmap, HashMap subjmap)
```

This method allows for flexible session based access control and delegation

- AuthzToken is used as session credential intra-domain and supports basic delegation scenarios
  - session (i.e. path creation) can be started privileged use e.g. researcher
  - if token is valid, all other users can perform their allowed actions
  - different scenarios may limit scope of session based delegation, e.g. only own domain, etc.

Method#8 - intra-domain session initiation and simple delegation (can issue session credentials of different token/ticket types)

```
String authorizeActionSession (String authzToken, String grireq,
  int delegtype, int sescred, HashMap resmap, HashMap actmap,
  HashMap subjmap)
```

Method #9 - Extends method #8 for inter-domain reservation/access control scenario (including simple delegation)

```
String authorizeActionSession (String authzToken, String griReq,
  int delegtype, int sescredtype, boolean renew, HashMap resmap,
  HashMap actmap, HashMap subjmap)
```

Returns:

- renewed session/AuthzToken if renew = (1,2) or token=null and requested sescred supported
- or string "Permit" or "Deny" depending on PDP decision

Future developments

- Combining network and Grid resources into one provisioning and AuthZ workflow/session
- Developing trust model for NRP
- Defining network topology aware XACML-NRP policy model
- Extend AuthZ session management model including related AuthZ ticket functionality and XACML policy model to support multidomain reservation process and (restricted) delegation
- Extending support for different user and resource profiles used in major Grid middleware frameworks and GN2/NRENs eduGAIN AAI
- Investigate using Identity Based Cryptography (IBC) for cross-domain trust relations management

Discussion and Questions