GAAA-AuthZ/GT4-AuthZ Gap analysis
or
Authorisation for Complex service provisioning and Collaborative applications

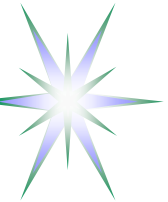
AuthZ Workshop Panel, GGF16

16 February 2006, Athens

Yuri Demchenko <demch@science.uva.nl>

System and Network Engineering Group

University of Amsterdam



Main topics

- Bootstrapping – Answering some workshop's topics and concerns
- Gap analysis: scope and document
- GT4-AuthZ as basic AuthZ platform for Grid and Web Services based applications
- GAAA-AuthZ extensions and planned addition to GT4-AuthZ
- Building compatibility and interoperability based on common AuthZ framework

Answering some workshop's topics and concerns

- LCG: Authorised session notion in Proxy containing VOMS credentials is rather identity based session
  - no action, or capability, and no resource and policy reference

  => Generic AuthZ ticket and Session management
- Biomed: Fine-grained access control with ACL
  - ACL always contains local security and resource context

  => Will benefit from separately managed policy explicitly defining Resource
- DK: "When security is too hard, people turn it off!"

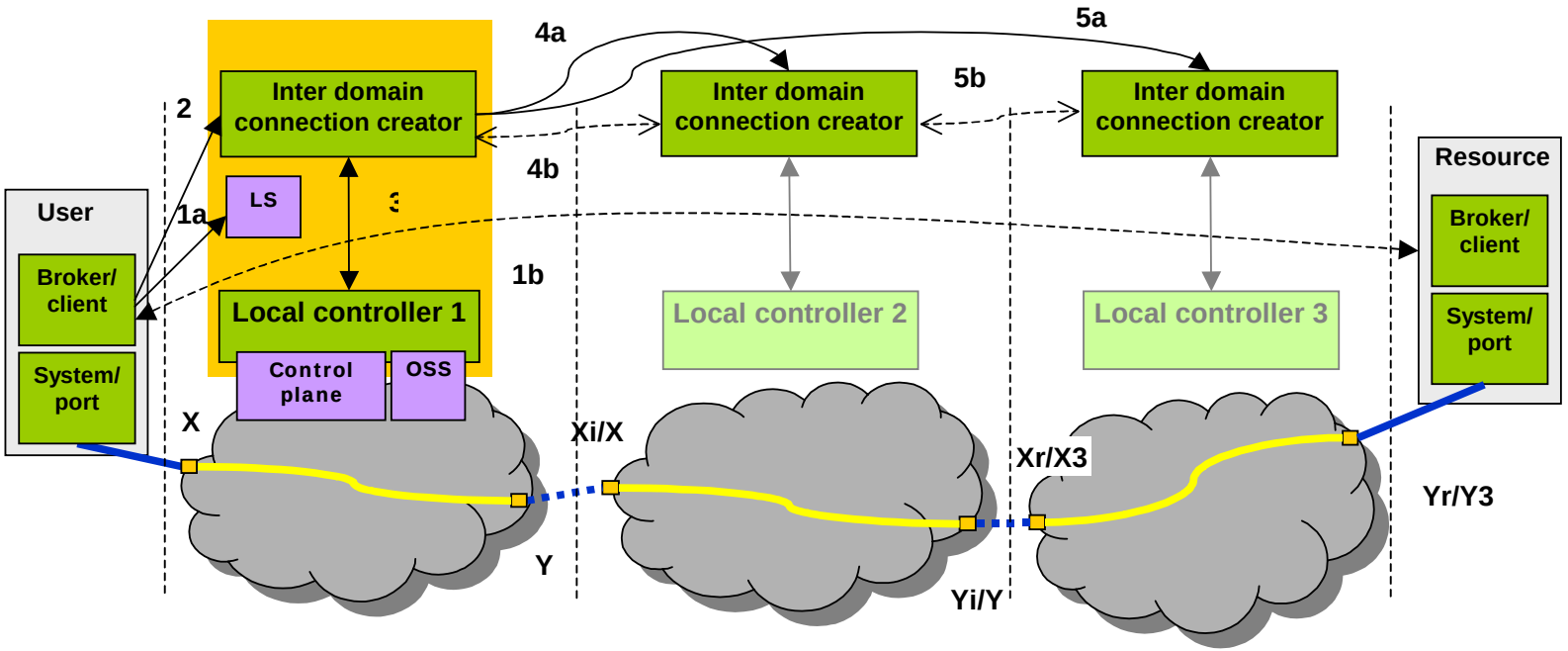
  => "When implementing/debugging security solution is too hard, developers will do it in their own way"

Gap analysis – Scope and document

- Two use cases and related requirements to AuthZ service
  - OLP provisioning as an example of complex resource provisioning (OLPP)
  - Grid based Collaborative Environment/applications (GCE)
- Analysis of existing solutions for Authorisation and related services
  - GT4-AuthZ , Acegi, GAAA-AuthZ
  - Attributes and security associations management: Shibboleth, VO and VOMS
  - Workflow management and driving policies
- Extending GAAA-AuthZ framework

- Document location (temporal):
  Filling the Gap with GAAA-P: Gap Analysis of Authorisation technologies and solutions for Optical Light Path Provisioning – Gigaport-NG RoN Technical report.
  Yuri Demchenko , Leon Gommans, Bas van Oudenaarde.
  http://staff.science.uva.nl/~demch/analytic/airg-gp6-ron-gap-aaa-12.pdf

OLP provisioning operation – Simple multidomain model



Step 1. The application broker or user client requests from the lookup services (LS) a path to a target system or resource

Step 2. Building/calculation of the interdomain connection between User and Resource domains with specific parameters

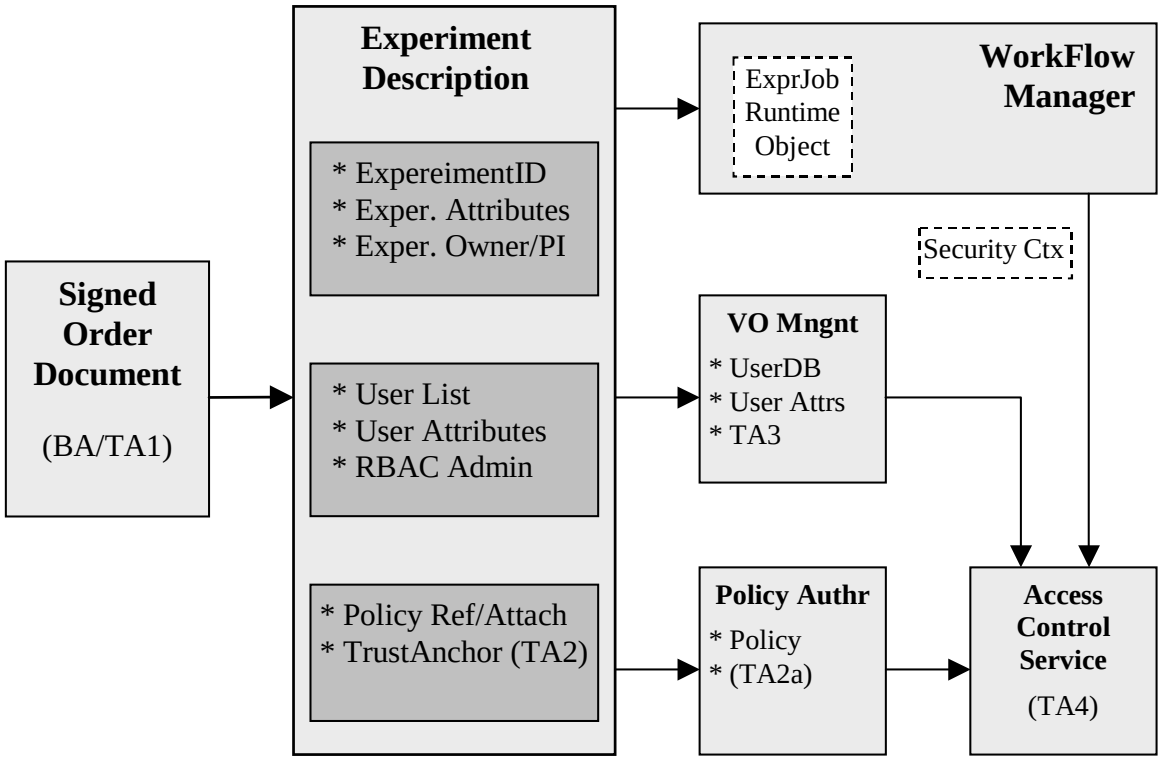
Step 3. Reservation of calculated path

- Agent based allocation
- Hop-by-hop allocation

Step 4. Provision reserved OLP

- Reservation ticket is used
- Fall-back conditions

Workflow and security context in GCE



Workflow manager drives an experiment and provides changing security context to Access Control service

- Adds stateful service and security context management to stateless Web Services

Collaboratory.nl project example

- Enterprise
- Facility/Instrument
- Virtual Lab
- Experiment/Instrument
- Stages
  - Setup
  - Experiment
  - Data processing
  - Reporting

Extending GAAA Authorisation Framework for OLPP and GCE

- GAAA AuthZ framework – two basic profiles are defined
  - GAAA-RBAC for Collaborative Environment
  - GAAA-P for interdomain network/resource provisioning
- Major GAAA-P components/extensions
  - Workflow control in the GAAA based provisioning model
    - WSFL and WSBPEL as upper layer to (stateless) WS/WS-Security
  - Dynamic trust management using federated trust model
    - Based on dynamic VO federation model
    - Compatibility with GridShib-SAAS
  - Attributes and metadata resolution and mapping
    - Support of common naming scheme and resolution
  - Policy combination and aggregation
    - For complex multi-component and multidomain resources
    - For combined policy audit/evaluation

GT4 Authorisation Framework

- Can potentially be configured for Container, Message, Service/Resource
  - But all based on SOAP/Axis message processing
- Authorisation is tied to SOAP message processing by Axis interceptor
- AuthZ processing sequence includes
  - Bootstrapping X.509 PIP – retrieves request parameters from the message
    - Subject, Resource, Action
  - Sequence of pre-configured PIP's, including SAML
  - Sequence of (specialised) PDP's
  - AuthZ engine combines PDP decisions using one of combination algorithms
- Available PDP's
  - ACL and GridMap
  - HostAuthorization and UserNameAuthorization
  - SAML AuthZ callout and SAML AuthZ Assertion
  - SelfAuthorization – based on shared/trusted Resource credentials
  - Simple XACML PDP (provided as a placeholder for extension)

Extending GAAA Toolkit - Adding new functionality to GT4-AuthZ

- Specific functionality provided by GAAA-AuthZ Toolkit
  - Authorisation Session handling
  - Authorisation tickets and tokens handling for performance optimisation
  - Complex XACML policies evaluation to provide fine-grained access control
  - Flexible trust domains and request/attributes semantics configurations and management

- Integration with GT4 and gLite Authorisation Framework
  - Using GT4 WS/messaging firmware to provide WS-based access to GAAA_tk authorisation service, to allow easy GAAA_tk integration into different applications
  - Adding GAAA AuthZ callouts to GT4/gLite AuthZ framework; this will allow using GAAA RBE as one of regular services for GT4 and gLite
  - Integrating GAAA AuthZ/RBE into GT4 AuthZ framework as one of PDP's

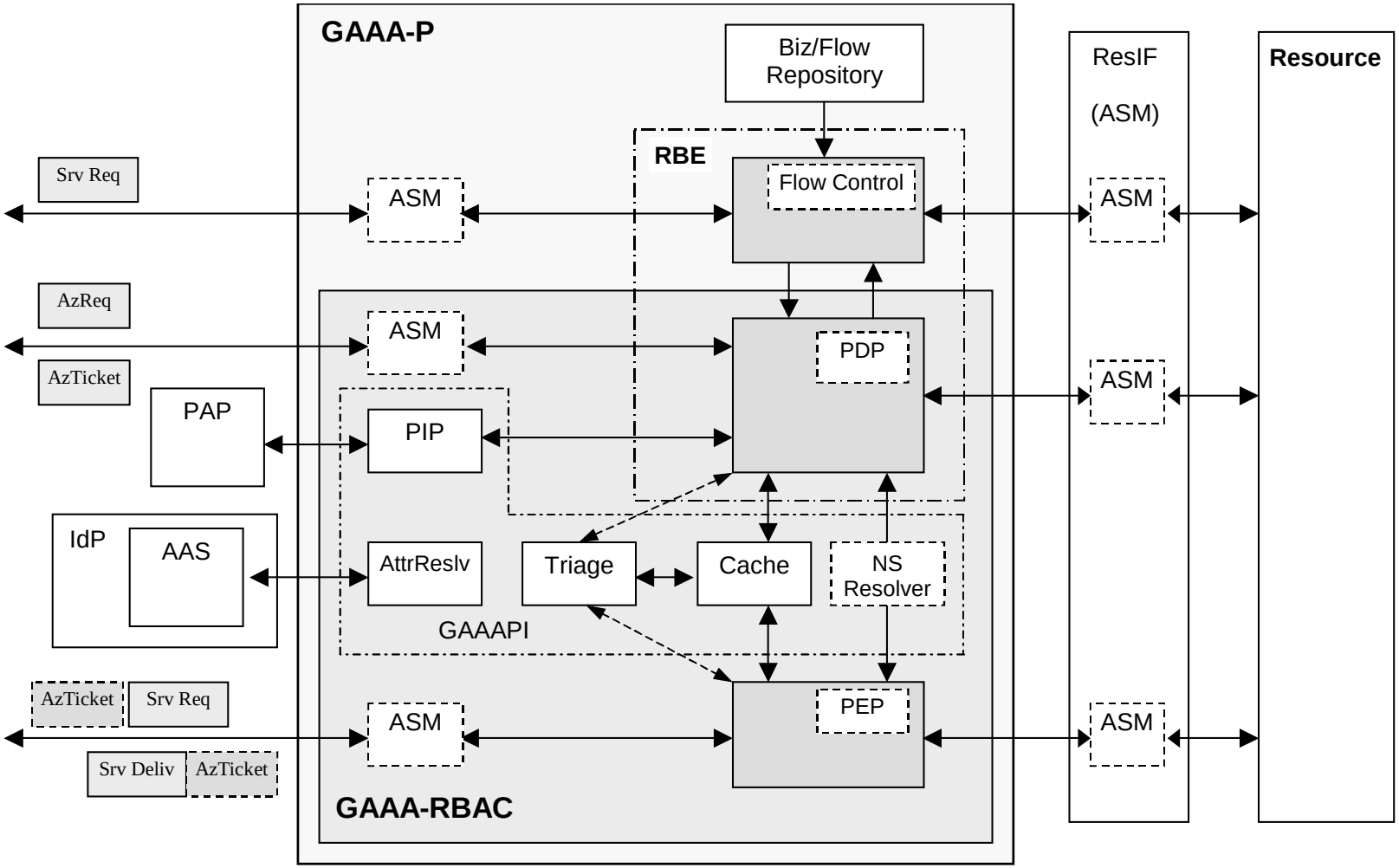
Building compatibility and interoperability based on common AuthZ framework

- Using, learning and promoting GT4-AuthZ
- OGSA-AuthZ Working Group
- Mapping between different AuthZ frameworks
- XACML policy format as a way to interchangeable policies
- Common or mapped attributes semantics

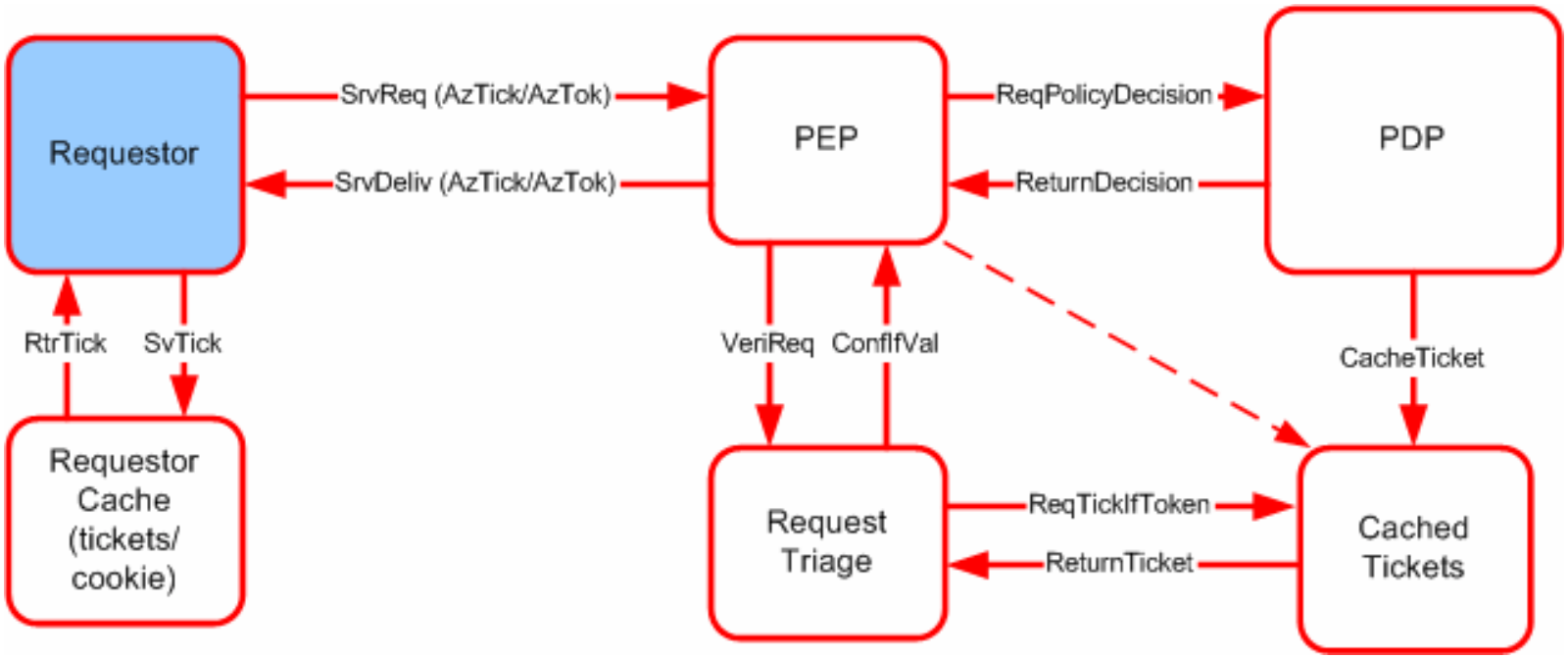
Additional information and graphics

- Extended GAAA Toolkit structure
- Tickets/Tokens handling with Triage
- Authorisation in complex Resource/Service
- Authorisation in GCE

Extended GAAA Toolkit structure

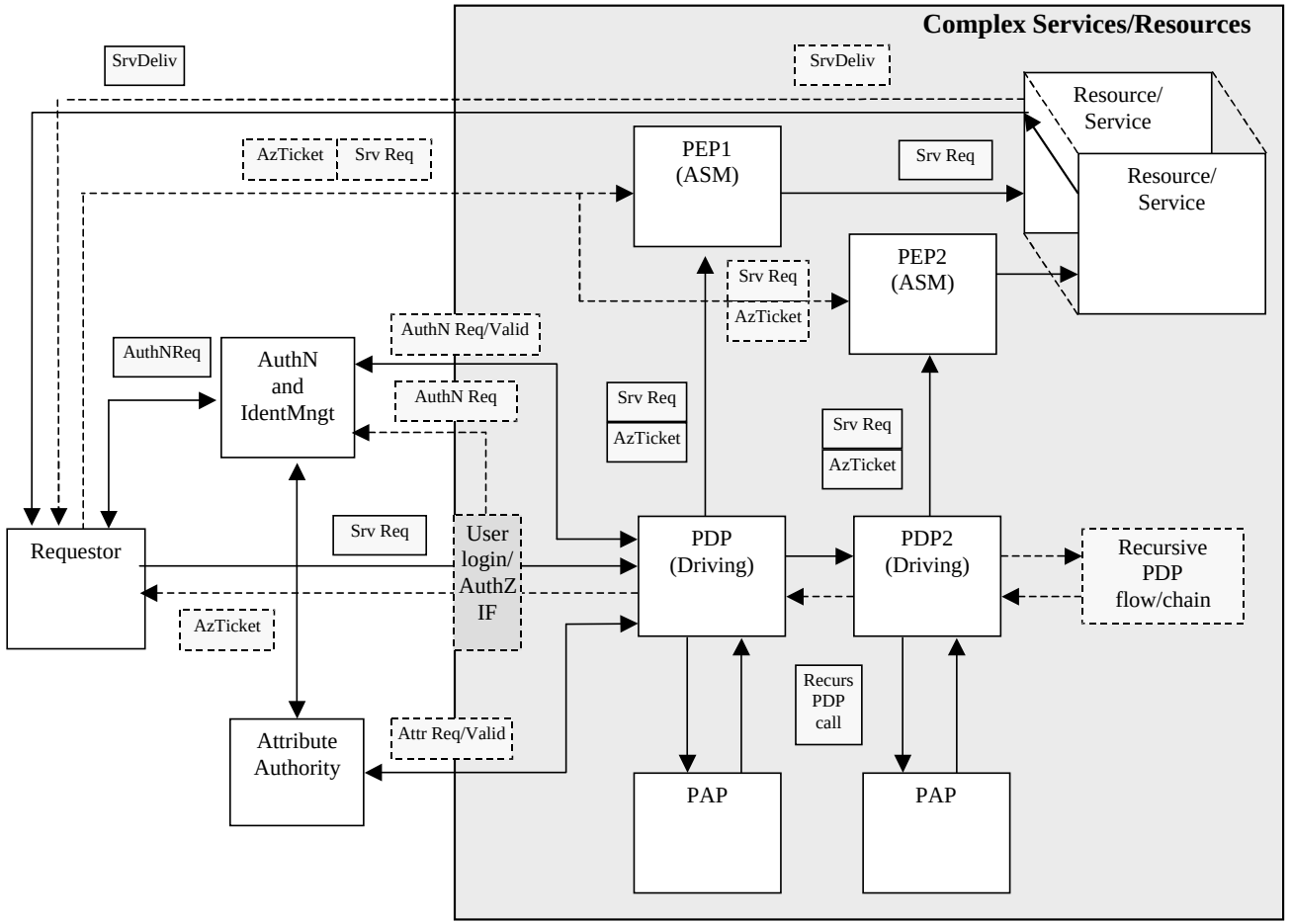


Tickets/Tokens handling in AuthZ system



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

Authorisation in complex Resource/Service



- Complex/multi-component resource
- Combined push and agent model

Authorisation in GCE