PHOSPHORUS

Information Society Technologies

LAMBDA USER CONTROLLED INFRASTRUCTURE FOR EUROPEAN RESEARCH

WP4: Authentication, Authorisation, Accounting (AAA)

The purpose of WP4 is to define the architecture and subsequently design, implement and test an AAA infrastructure to support policy based on-demand optical Network Resource Provisioning (NRP) and access across different administrative domains.

The proposed solutions should ensure interoperability and integration with currently used and developing Grid AAA/AuthZ solutions.

GAAA-NRP Authorisation infrastructure for on-demand NRP

The typical on-demand network resource provisioning process includes four major stages, as follows: (1) resource reservation; (2) deployment (or activation); (3) resource access/consumption, and additionally; (4) resource de-commissioning after it was used.

In its own turn, the reservation stage (1) typically includes three basic steps: resource lookup; complex resource composition (including alternatives), and reservation of individual resources. The reservation stage may require the execution of complex procedures that may also request individual resources authorisation. At the deployment stage, the reserved resources are bound to a reservation ID, which we refer as the Global Reservation Identifier (GRI).

GAAA-NRP security mechanisms

The GAAA-NRP AuthZ infrastructure provides the following access control mechanisms and components that extend the generic GAAA-AuthZ model described in RFC2904 with the specific functionality for on-demand NRP:

- AuthZ session management to support complex AuthZ decision and multiple resources access, including multiple resources belonging to different administrative and security domains.
- Policy obligations to support usable/accountable resource access/usage and additionally global and local user account mapping widely used in Grid based applications and supercomputing.
- AuthZ tickets with extended functionality to support AuthZ session management, delegation and obligated policy decisions.
- Access and pilot tokens used for interdomain reservation process management access control as part of the policy enforcement mechanisms that can be used in the control plane and in-band.

The solutions proposed in the GAAA-CRP framework are based on using such structural components and solutions as the Token Validation Service, the Obligation Handling Reference Model (OHRM), and the XACML attributes and policy profile for multidomain NRP (XACML-NRP profile)

[RFC2904] RFC2904 "AAA Authorization Framework", August 2000. ftp://ftp.isi.edu/in-notes/rfc2904.tx
[XACML-NRP] "GAAA Toolkit pluggable components and XACML policy profile for ONRP", Phosphorus Deliverable D4.3.1, Sept. 30, 2008. http://www.ist-phosphorus.eu/files/ deliverables/Phosphorus-deliverable-D4.3.1.pdf
[XACML-Grid] "An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids," Joint EGEE, OSG, and Globus document. https://edms.cern.ch/document/929867/1
[GAAA-TK] "GAAA Toolkit library for ONRP (final project release)", Phosphorus Deliverable D4.5, March 30, 2009. http://www.ist-phosphorus.eu/files/ deliverables/Phosphorus-deliverable-D4.5.pdf

Token Based Signalling and Access Control in multidomain NRP

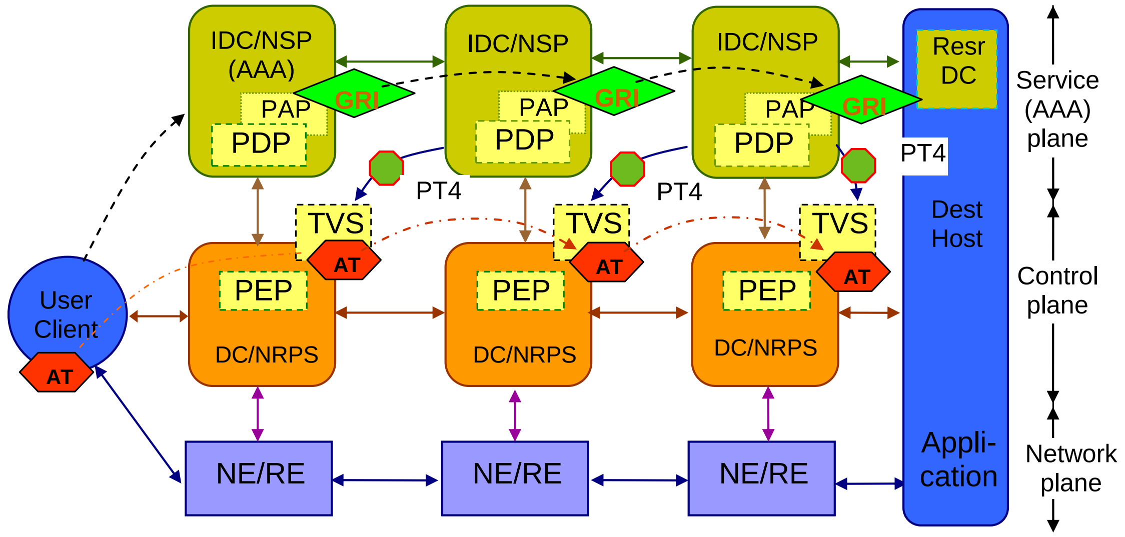

Figure 1. Components involved in multidomain network resource provisioning.

CRP stages reservation, deployment and access are presented by the flows correspondingly GRI (forward from the user to the resource), pilot tokens PT4 (backward), and access tokens AT (forward).

The XML and binary tokens are used for signalling and access control at different NRP stages as a mechanism for communicating security context between domains and are used as the provisioning or AuthZ session credentials:

The token handling functionality is outsourced to the Token Validation Service (TVS) that supports different token handling models and store token and session related context. Basic TVS functionality allows checking if a service/resource requesting subject or other entity, that possess current token, has permission to access/use a resource based on advance reservation to which this token refers. During its operation the TVS checks if a presented token has reference to a previously reserved resource and a request information conforms to the reservation condition.

GAAA-NRP Implementation in the GAAA-TK Pluggable Java Library

All proposed GAAA-AuthZ functionality is currently being implemented in the GAAA Toolkit (GAAA-TK) pluggable Java library in the framework of the Phosphorus project.

The GAAA-TK library allows for AuthZ request evaluation with the local XACML based PDP or calling out to the external AuthZ service using the SAML-XACML protocol. Current library implementation supports both XACML-Grid and XACML-NRP profiles.

The GAAA TK library provides few PEP and TVS methods that support extended AuthZ session management and provide necessary AuthZ token and ticket handling functionality.

The TVS component is implemented as a part of the general GAAA-TK library but can also be used separately. It provides all required functionality to support token based policy enforcement mechanism that can be used at each networking layer and in particular for token based networking.