

Building a Multi-Domain Grid

by Freek Dijkstra and David Groep

Joining resources from different administrative domains is currently a nightmare, but the problem may be alleviated with local and global authorization systems developed by the Dutch high-energy physics institute NIKHEF and the University of Amsterdam (UvA). By combining generic authentication, authorization and accounting (AAA) service techniques and site-local authorization, the creation of a 'virtual organisation' can become more dynamic and easier for both users and administrators.

It is expected that as the Grid matures, user communities will become more dynamic, shorter-lived, and based on detailed policies rather than binary access decisions. Policy-based coordination of all resources, and minimal per-resource configuration is therefore essential.

Currently, most Grid infrastructures use as their core authorization system GSI, the Grid Security Infrastructure developed by the Globus Alliance. GSI is based around the Public Key Infrastructure concept, where trusted third parties issue certificates to both users and resources. In plain GSI, access rights are directly linked to the user's identity. The resource provider keeps a list (grid-mapfile) of names of authorized users, and associates local accounts with these users. However, it is necessary to make the mappings in advance, as the grid-mapfile is maintained locally at each resource.

Unfortunately this does not scale well, since the grid-mapfile must be updated continuously as users are added to the community or 'virtual organization' (VO). It is also prone to privacy problems, since it forces one to publish a list of all users in a project to all partners, even if the user never intends to use a specific resource.

Local Credential Mapping

The local authorization services developed by NIKHEF mitigate these problems. The new model is based on the Virtual Organization Management Service VOMS, an authorization-attribute service developed in the DataTAG project by the Italian nuclear physics institute INFN. Access controls are no longer bound only to the user's

identity, and decisions can be based on attributes issued to the user by the VO. The only infrastructure needed to establish a VO is this attribute authority, and at the local resource a single line of configuration suffices both to enable access for the new community and to support fine-grained policy controls defined and implemented by the VO.

Recently, the Virtual Laboratory for e-Science project in the Netherlands adopted this model for enforcing access controls to data sets spread across two hospitals, a research institute and the national computer centre.

The site aspect of the system implemented by NIKHEF consists of two parts: the Local Centre Authorization Service (LCAS) and the Local Credential Mapping Service (LCMAPS).



Apart from computing services, users may want to provision dedicated network services at the same time.

LCAS is a policy-decision module for implementing site-access policies, where the policies can be changed at run-time. It is currently a key element in enforcing security policies in many production systems, enabling site security officers to limit damage caused by compromised identities.

However, access control to the resource as a whole is not sufficient. LCMAPS, which can parse VOMS attributes, can dynamically assign specific Unix groups to fine-grained attributes. These groups are then linked to an unprivileged account for execution. The translation from VOMS attributes to Unix groups is performed on the fly. Wildcard VO group specifications give the site control over the number of Unix groups assigned to an individual VO. Sandboxing is thus achieved inside any existing Unix system.

LCMAPS supports a variety of ways to collect VO information from traditional user-proxies, VOMS attributes and grid-mapfiles, and a wide variety of account-enforcement modules for both single machines and clusters of computers.

Multiple Resources

Computing and storage are only part of the picture however, with new resource types such as remote instruments and optical networks joining the grid. This poses new challenges for resource brokers when independent organizations are involved.

Wide-area networks in particular have many different stakeholders. Packets travelling from NIKHEF in Amsterdam to, say, the Lawrence Berkeley lab in San Francisco will encounter five different providers. With valuable resources such

as optical networks - your own personal light path from A to B - access control and dynamic authorization are sine qua non in the commercial world. Consequently the user running a calculation in Amsterdam, with the data in San Francisco, will need both of these resources simultaneously.

The AAA server, developed by the University of Amsterdam, fills this gap in traditional resource management. The AAA server is capable of taking authorization decisions across domains, and uses policy files to determine business logic. It can, based on the current policy,

contact other services to fulfill users' requests. The attributes themselves may in fact be issued by the VOMS server, thereby seamlessly integrating network, storage and computer access.

The University of Amsterdam (UvA) has already demonstrated that the AAA server is able to make authorization decisions involving the provisioning of a dedicated network connection, even if the connection crosses multiple domains.

Now, the UvA and NIKHEF have joined forces to build a role-based authorization

system for the European Grid Infrastructure, deployed by two projects: Enabling Grids for E-science in Europe (EGEE) and the Dutch Virtual Laboratory for e-Science (VL-E).

Links:

<http://www.nikhef.nl/grid/>

<http://www.science.uva.nl/research/air/>

Please contact:

Freek Dijkstra, Universiteit van Amsterdam, The Netherlands

Tel: +31 20 5257531

E-mail: fdijkstr@science.uva.nl

David Groep, NIKHEF, Netherlands

Tel: +31 20 592 2179

E-mail: davidg@nikhef.nl

Resource Management in an Optical Grid Testbed

by Helmut Grund and Wolfgang Ziegler

The German Ministry for Research and Education (BMBF) launched the Vertically Integrated Optical Testbed for Large Applications (VIOLA) project in spring 2004. The project is managed by 'Deutsches Forschungsnetz' (DFN) and will run for three years.

Emerging new technology for optical networks will deliver QoS and bandwidth far beyond the capacity and capabilities of today's networks. For the evaluation of new network components and architecture, the integration of network techniques and applications has proven a success in former testbeds. The technical basis of the testbed is comprised of optical network components connecting compute resources, from which a grid based on the UNICORE system is built

up. To allow large complex applications stressing the capabilities of the underlying optical network, additional grid components will be adopted, including a MetaScheduler (allowing co-allocation of compute resources, network resources with the necessary QoS or other resources like visualization devices) and MetaMPICH communication libraries for distributed applications using MPI for interprocess communication.

The expected outcomes of the project are threefold. First, new network techniques will be deployed and tested in an optical testbed, and along with ambitious applications will provide know-how for future generations of networks, especially the next generation of the German NREN X-WIN. Second, the enhanced Grid middleware originating from the project will become useful in the German e-Science Initiative D-Grid. The third important aspect of the project is the collaboration with other projects on a national, European and international level.

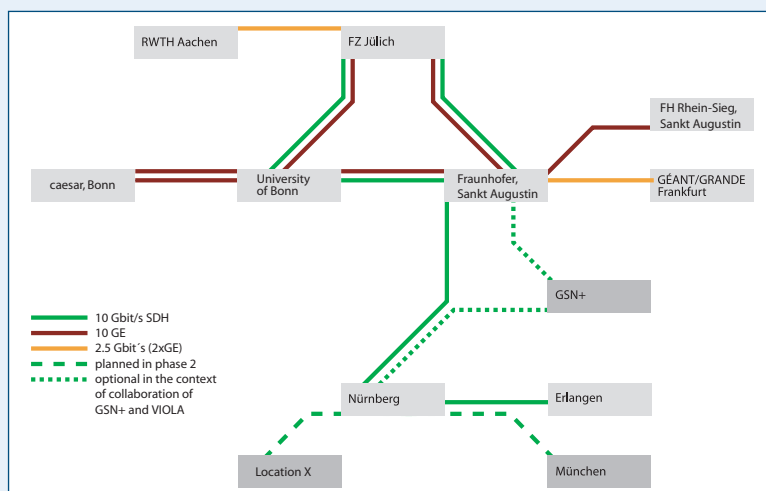


Figure 1:
VIOLA
Testbed
Topology.

The consortium of the project is led by the DFN, ranges from research institutes and universities to the telecommunication industry, and includes Research Centre Jülich, Fraunhofer Institute for Scientific Computing and Algorithms (SCAI), Fraunhofer Institute for Media Communication (IMK), the Centre of Advanced European Studies and Research (CAESAR), RWTH Aachen University, Bonn University, the University of Applied Sciences Bonn-