

SECOND TERENA NREN-GRIDS WORKSHOP FOCUSES ON AAI

TERENA hosted the second NREN-Grids Workshop on Monday 17 October 2005 in Amsterdam. The meeting was attended by more than 50 delegates representing National Research and Education Networks (NRENs), Grid projects and industry.

In its annual meeting in Poznań in June 2005, the TERENA Technical Advisory Council re-affirmed Grids as Special Interest Area for the coming two years. TERENA aims to provide general information about Grid-related activities and projects in Europe and worldwide such as the Global Grid Forum (GGF), as well as to provide links to information on Grid-related topics and TERENA initiatives. TERENA's role is mainly as liaison between the European Research Networking community and the Grid communities. To this end, one-day NREN-Grids workshops are being organised by TERENA on a regular basis.

In 2005, TERENA hosted two NREN-Grids Workshops (which are open to the NREN and Grid communities) to discuss and evaluate the implications of Grid Services on network provision. The aim is to reach a common understanding about the likely impact of Grids on NRENs and to be ready to deliver the appropriate services.

The first NRENs-Grids Workshop was held on Thursday 12 May 2005, in Amsterdam and discussed and evaluated the implications of Grid services on network provision from an NREN perspective. It was agreed to include more input from the Grid community in future meetings so that members of the NREN and Grid communities could update one another and reach common understandings.

The second NREN-Grids workshop in October focussed on Authentication and Authorisation Infrastructure (AAI). Deterministic Schedulable End-to-End Pipes were also explored.

The objectives of the day were to:

- **Exchange information on current practice**
- **Reach a common understanding about the likely impact of Grids on NRENs**
- **Compile a list of potential action points**

John Dyer, TERENA's Chief Technical Officer outlined current TERENA activities relevant to AAI. He introduced the new 'refeds' (Research and Education Federations) email distribution list which has been created to discuss the issues of federations and federations of federations (confederations). He mentioned other related AAI activities in TERENA including TACAR (Anchor of Trust), TF-EMC2 (Collaboration & Coordination), TF-Mobility (Roaming) and EuroCAMP (Campus Architecture Middleware Planning Workshops).

Klaas Wierenga of SURFNet (Netherlands) provided a view of the AAI domain from the NREN perspective. The current situation is one of several fragmented solutions with separate systems for network access, system and

web-logins. As diversity has grown, there is an increasing desire to rationalise into a single solution that will work across all systems. The concept of federations and indeed federations of federations (now termed confederations) seems to offer a way forward. Eduroam has demonstrated a good model of how federations can operate displaying important elements such as how to transport users' attributes in a safe manner.

Scaling from the present low numbers of Grid users to a pervasive system that can identify and authenticate large numbers of users is a big issue. If the academic and research community works together with the NREN community effectively, a viable solution will be found.

In his presentation on NRENs supporting Grids using current Grid technology, Milan Sova of CESNET explained that in his opinion, the development of Public Key Infrastructure (PKI) has not had a good record of success, with several false starts. There are many reasons for this, including the complicated nature of the implementation of the Globus Toolkit. However, there have also been some notable successes in the PKI space, specifically that of EUGridPMA which coordinates the accreditation of more than 50 Certification Authorities (CAs) on three continents.

There may be difficulty to converge the NREN and Grid communities to use common CAs, due to the more stringent Grid requirements. However, the future may see the use of short-lived, rather than long-lived certificates as are used currently. Institutions and NRENs should dedicate some full-time resources to address the issue of developing coherent AAI architectures and systems.

Christoph Witzig of SWITCH (Switzerland) reported on a proposal that is currently under consideration by the European Commission to integrate AAI with Grid in the EGEE-2 project. Briefly, SWITCH will develop interoperability of Shibboleth/gLite for the EGEE-II project, should the proposal be accepted. While Grid is a new direction for SWITCH, they currently have 110,000 AAI-enabled email accounts which represents about half of all their users. They therefore have some valuable practical experience in the provision of AAI. He stressed the position of the institutions as being the users' identity providers and there was some discussion regarding the privacy of user attributes.

Christos Kanellopoulos of AUTH (Greece) pointed out that AAI is far from mature and he provided an indication of common characteristics that should be incorporated. The central theme is that the AAI must be capable of providing a definitive electronic identity for the user and his roles. The role may be either allocated by pull (the user requests it from the administration) or push (in which the user is automatically given a role by the administration). Whichever approach is adopted, the objective should be to make the life of the user as easy as possible. Institutions and virtual organisations that are large will not be able (or want) to manage the allocation of identities from a single central point and therefore any system that is put in place must be capable of supporting delegation. The use of eXtensible Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML) will likely be useful in implementing practical solutions.

Jean-Marc Uzé of Juniper Networks introduced the topic of Schedulable Deterministic End-to-End Pipes (SDE2EP) which are connections offering guaranteed bandwidth, delay, and jitter, and no packet-loss, frame-loss or reordering. Whilst it is possible to conceive of SDE2EPs being supported by techniques at Levels 1, 2 and 3, some experts believe that only L1 solutions can provide true SDE2EPs, and some others believe that a hybrid model would open more opportunities (ubiquity). Whatever the solution is, there is a need for a Capacity Management Middleware.

Several initiatives in Research and Education (R&E) community are developing such tools. However, there are number of challenges to be addressed, not least, the licensing and interoperability issues. A major objective is to select and converge on a single and global solution for R&E. Jean-Marc's wish list of characteristics for SDE2EPs includes: Ubiquity; Platform/Vendor independence and domain independence. They should also be persistent and federative, and potentially reusable for other on-demand services.

A model proposed by the IPsphere Forum includes the concept of a business layer, based on Service-Oriented Architecture (SOA)/ Web Services (WS) principles for the exchange of business information, making it easy for it to manage the elements of higher-layer services that require identity management and reliable communications, including Grid computing and ASP services, across multiple operators.

In conclusion, the development and deployment of SDE2EPs will require vertical and horizontal approaches and synergy between the NREN and Grid community, but also with industry.

Licia Florio of TERENA summarised the main points of the presentations:

- Federations (of Trust) are becoming increasingly important in both the NREN and Grid communities;
- Convergence between the NREN and Grid AAI spaces is generally agreed to be possible;
- The question of whether future AAI systems will need to use technologies in addition to certificates should be explored;
- There are many approaches to providing AAI already in place;
- There are AAI scalability issues to be faced in the future.

Some current community initiatives in the NREN community might help the Grid community:

- TACAR – The TERENA anchor of trust for community Certification Authorities;
- The Server Certificate Service Pilot which can help by providing server certificates that are automatically recognised by common browsers;
- The integration of Shibboleth with Grid software;
- Collaboration between eduroam and EUGridPMA on exchanging details of accredited federations;
- Convergence of identity providers Schemas in the campuses and Virtual Organisations using the work of SCHAC (the TF-EMC2 subgroup on schema extensions).

In order to make the collaboration between Grids and NRENs more fruitful, there needs to be some in-depth discussions on Grid Networking and AAI requirements, Experience on using MyProxy credential repository for storing user keys and the Management of Federations.

The meeting concluded that identifying AAI technical solutions is relatively straightforward. It will be much more challenging to reach consensus on the administrative and legal agreements between federations. A major issue will be data privacy, particularly in respect to the exchange or exposure of attributes. Whilst it may be possible for NRENs and other national organisations to agree on national policies for shipping attributes, the

situation of international Virtual Organisations (VOs) is somewhat more complex. VOs typically cross national boundaries and may be subject to several national (and possibly different) policies. It is therefore essential that a suitable forum be identified in which common agreements can be made. Several delegates thought TERENA could provide a neutral forum in which such discussions could take place and agreements be made. The e-Infrastructures Reflection Group white paper was also mentioned in this context.

While current AAI systems are capable of supporting small numbers of long-lived federations, support for large numbers of federations and short-lived virtual organisations are beyond their capabilities. One delegate suggested that there will be a potentially large demand to support very many short-lived and small project or contract-based VOs. These might consist of just a few people (less than ten) and last six months or less.

It is commonly agreed that VOs need be little more than a directory containing information about the resources and users. There must be some mechanism for users to register the resources they are contributing to the VO so that the VO can make this information available to other users. Additional problems arise in cases when short-lived certificates expire before a job has used its authentication to claim the resources it needs to complete its task as well as in delegation and in the use of Shibboleth and Single Sign-On (SSO).

DEISA reported that they use UNICORE-based middleware that does not rely on proxy certificates, but authorises users directly and then provides access to the appropriate server. Some delegates thought that having a dedicated server managing users a good solution.

There is a need to clearly distinguish between the trust that can be developed between individuals and trust that models that are needed between institutions. The issue of whether institutions will want to allow attributes to travel outside of their own management domain was also raised. There is a need to be able to trace every instance of granting of rights and a need to keep records of these events. It was suggested that the required persistence of records can only be achieved through long-lived (permanent) organisations, which is rather at variance with the concept of short-lived VOs. It was suggested that even short-lived VOs receive their resources from long-lived organisations so maybe the problem is not insurmountable.

Finally, the need for VOs was agreed. Having thousands of scientists working in many sites spread over many countries requires that all users to be registered at all sites. This is clearly unscalable. The alternative is using a robust and auditable policy-based procedure so that each of the users needs to be registered just once in a VO and all sites are given read-only access to the authorisation data.

The next NREN-Grids workshop will be held in six month's time (March/April 2006). The plan is to actively invite campus administrators to participate in the event in order to discuss issues of user registration.

A meeting report on the second workshop and background information about TERENA's NREN-Grid activities can be found at:

<http://www.terena.nl/tech/grid/nren-workshop.html>



TRANS-EUROPEAN RESEARCH AND EDUCATION NETWORKING ASSOCIATION
For more information, please contact the TERENA Secretariat
Tel: +31(0) 20 530 4488, email: news@terena.nl