

TERENA 2nd NREN-Grids Workshop

Meeting Report

John DYER
27 October 2005

Introduction

TERENA hosted the 2nd NREN-Grids Workshop on Monday 17th October 2005 in Amsterdam. The purpose of the event was to discuss and evaluate the implications of Grid services on network provision in the NREN community with a particular focus on Authentication and Authorisation Infrastructure (AAI). Deterministic Schedulable End-to-End Pipes were also explored. The meeting was attended by more than 50 delegates representing NRENs, Grid projects and industry.

The objectives of the day were to:

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

The meeting was opened by John Dyer who explained the current TERENA activities that have relevance in the AAI space. 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). Work in the refeds group builds on the technical issues raised in the Cotswold Group meeting that took place in October 2004. Individuals actively working on planning, development or operation of federations are invite to join the group be emailing him at John.Dyer@terena.nl. He also mentioned:

- SCHAC Schema extensions
- TACAR Anchor of Trust
- TF-EMC2 Collaboration & Coordination
- TF-Mobility Roaming
- EuroCAMP * Campus Architecture Middleware Planning Workshops

* The 2nd TERENA EuroCAMP takes place in Porto, Portugal, 7-9 November

Five presentations to inform discussions were provided:

- Global inter-working AAI
 - AAI from the NREN perspective - Klaas Wierenga, SURFnet, NL
 - NRENs supporting Grids using current Grid Technology - Milan Sova, CESNET, CZ
 - Perspectives of Integrating AAI with Grid in EGEE-2 - Christoph Witzig, SWITCH, CH
 - NRENs, Grids and Integrated AAI - Christos Kanellopoulos, AUTH, GR
- Schedulable deterministic end-to-end pipes
 - Jean-Marc Uze, Juniper Networks

During the afternoon there was an extended discussion session in which issues raised in the presentations and potential solutions were discussed.

Authentication and Authorisation Infrastructure (AAI)

*AAI from the NREN perspective
Klaas Wierenga, SURFnet, NL*

Klaas Wierenga provided a view of the AAI domain from the NREN perspective. He suggested that 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. Klaas explained that 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. He went on to explain the elements of the eduroam architecture including the RADIUS hierarchy, trust elements and shared secrets.

Klaas explained that 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. He believes if the academic and research community works together with the NREN community effectively, a viable solution will be found.

*NRENs supporting Grids using current Grid Technology
Milan Sova, CESNET, CZ*

Milan explained that in his opinion that the development of PKI has not had a good record of success with several false starts. He cited many reasons for this including the complicated nature of the Globus Toolkit implementation. However he also mentioned some notable success in the PKI space, specifically that of EUGridPMA which coordinates the accreditation of more than 50 CAs on three continents.

There is a view that there may be difficulty converging the NREN and Grid communities to use common CAs due to the more stringent Grid requirements. Milan does not hold this view. He explained his view that the future may see the use of short-lived, rather than the long-lived certificates as are used currently. He called for institutions and NRENs to dedicate some full time resources to address the issue of developing coherent AAI architectures and systems.

*Perspectives of Integrating AAI with Grid in EGEE-2
Christoph Witzig, SWITCH, CH*

Christoph reported on a proposal that is currently under consideration by the European Commission. Briefly, SWITCH propose to develop Shibboleth/gLite interoperability for the EGEE-II project should the proposal be accepted. Christoph went on to explain that whilst Grid is a new direction for SWITCH, they currently have 110,000 AAI enabled email accounts in Switzerland which represents about half of all 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. There was some discussion regarding the privacy of user attributes, a topic that was re-visited during the afternoon discussions.

NRENs, Grids and Integrated AAI
Christos Kanellopoulos, AUTH, GR

It is clear that AAI is far from mature and Christos 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. Christos explained that the role maybe 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. He also explained that 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. He suggested that the use of eXtensible Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML) will likely be useful in implementing practical solutions.

Schedulable deterministic end-to-end pipes
Jean-Marc Uze, Juniper Networks

Jean-Marc introduced the topic of Schedulable deterministic end-to-end Pipes (SDE2EP) which are connections offering guaranteed: bandwidth; delay; jitter; 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 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 service.

Jean-Marc explained a model proposed by the IPsphere Forum which 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. He explained the IPsphere reference architecture (compatible with current & emerging standards) in detail, in his presentation and slides.

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.

Summing up

Licia Florio of TERENA summarised the main points of the presentations. The main points were:

- 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.

Licia went on to explain ways in which the NREN community might be able to help the Grid community and mentioned some current community initiatives:

- 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.

It is clear that 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.
- Management of Federations.

Discussion Session

There was a general feeling that identifying AAI technical solutions is relatively straightforward. It will be much more challenging to reach agreement on the administrative and legal agreements between federations. A major issue in this space 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 is somewhat more complex. Virtual Organisation 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.

Whilst 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 10) and last 6 months or less.

There was a detailed discussion on the nature of VOs. There was a common view 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 discussed were: cases where short-lived certificates expire before a job has used its authentication to claim the resources it needs to complete its task; delegation; use of Shibboleth and 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.

It was suggested that 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. The issue of audit trails was also discussed, in particular the need to be able to trace every instance of granting of rights and the 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.

The need for VOs was questioned by one of the delegates. In response a representative of LCG and EGEE reported that they have thousands of scientists working in 200 sites spread over 30 countries. Using traditional a traditional login/password approach to give access of all researchers at all sites would require all users to be registered at all sites. This is clearly unscalable being an “n x n” problem. The alternative of using a robust and auditable policy based procedure, 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.

Actions

A number of urgent action items were identified:

REF	Action	Contributors
02/01	To undertake an analysis of the differences between NREN and Grid understandings of the issues.	Community Volunteers to discuss on the nren-n-grids email distribution list
02/02	Agreement on the necessary tools to support VOs	Discuss on TERENA refeds email distribution list
03/03	Development of a coherent set of recommendations on how to register tens of thousands of users	Community Volunteers to discuss on the nren-n-grids email distribution list

Next Workshop

The 3rd NREN-Grids Workshop will be held in six months time (March/April 2006) and the aim is to proactively invite Campus Administrators to participate on issues of user registration.

www.terena.nl/tech/grid/nren-workshop.html