

Open Workshop on e-Infrastructure (e-IRG Workshop)

Report

The open Workshop on e-Infrastructure was held at the Swiss Federal Institute of Technology (ETH) in Zürich, 24-25 April 2008.

The aim of this workshop was to discuss and explore open issues and questions for enabling an easy, secure and cost-effective shared use of distributed electronic resources across Europe and in collaboration with other international initiatives based on sustainable e-infrastructures. The e-IRG board evaluated - through expert consultation - the following topics as benefiting most from an open reflection and discussion:

- Security, a framework for Information Infrastructure Protection.
- Cyber infrastructures and e-Infrastructure initiatives.
- Virtualization: A new trend and its impact on research e-infrastructures.

The security topic addresses a fundamental and indispensable component of the e-Infrastructure that needs to be harmonized among the different key players at national and international level in order to achieve true global interoperability. As a contrast, the other two topics represent new aspects, opportunities and trends in the field of e-Infrastructure. For these new topics the principal aim was to introduce the contents and activities in order to assess the need for new initiatives in the e-IRG and the community it represents.

Security, a framework for Information Infrastructure Protection

As the security is an extremely important issue in the framework of e-Infrastructure, the whole first day of the workshop was dedicated to the topic. This allowed addressing not only the practical details and challenges in the area, but also the more fundamental obstacles stemming from the fact that the security is not an universally well-defined concept. As a result of this ambiguity, implementations and their central assumptions depend on the contexts and fields of application.

The aim of the session was to present the different perspectives of the main stakeholders in e-Infrastructure and - through a panel discussion - try to find a common ground as well as outline a general framework that incorporates the different views. Based on such a common framework it should be possible to harmonize and coordinate policies and developments more efficiently than before.

As an introduction, Thomas Dübendorfer from ISSS / Google presented ten top security trends. He stressed the new economic value of information, the question of controlling the information and its use, and listed critical infrastructure outages and misuses. Afterwards, four presentations, given by representatives of four major e-Infrastructure initiatives, provided an insight into policies, implementations and needs related to their fields of application.

The director of ARNES, the Slovenian NREN, who was also representing the Trans-European Research and Education Networking Association (TERENA), viewed security issues from the standpoint of the National Research and Education Networks (NREN). He stressed the importance of trust between different actors forming the research e-Infrastructures. Speakers representing Grids (EGEE III), supercomputers

(DEISA) and data infrastructure projects (EMBL) presented security models, solutions and challenges as seen from their respective perspectives. The presentations demonstrated clearly that in these distinct fields of activity the semantics and the meaning of the security as a concept are indeed quite different.

In the subsequent contribution, the Chief Security Officer of SWITCH presented a framework for Security and Identity Management as a basis for discussion in the subsequent round table discussion with all authors.

In general it was widely concluded that there is a need for an increased collaboration in Security and Identity Management between all involved communities at institutional, national and international levels.

Findings and recommendations

- NRENs and TERENA
 - NRENs have a well established and networked security organization for reactive and proactive activities through the TF-CSIRT at national and international level
 - NRENs manage authentication issues at national level for secure data networking at national and international level (PKI)
 - NRENs organize and provide authentication and authorization services (through the Authentication and Authorization infrastructure AAI) for federated identity management purposes at national and international level
 - A need for action has been identified in security and identity management issues between the nationally oriented NRENs and the project- or Virtual Organization-oriented Grids
 - The NREN community proposes its own hierarchical organization as a model for a sustainable Grid infrastructure in Europe (NGI, EGI)
- Grid represented by EGEE-III (and in a future EGI)
 - There are no standards on Grid security organization
 - The Grid Security Model is self-contained and based on certificates
 - The security organization is complex, encompassing different fields from middleware development and debugging; policy development and deployment and extending to the reactive and proactive cross-organisational operation at the international VO-level
 - In order to face the ever increasing security challenges, Grid Security needs, to consider
 - The national AAI based on federated identity, which offers the perspective of accessing a large user community
 - An increased collaboration with NRENs and their CERT/CSIRT at institutional, national and international levels
- Supercomputer represented by DEISA (and in a future PRACE)
 - The supercomputer field is represented by a relatively small community of highly specialized users with focused needs concerning security
 - The focal interest of DEISA is on performance in job management services and global data infrastructure
 - Security and identity management in DEISA should rely on dedicated high speed network infrastructure and common AAA infrastructure for the closed community
- Data infrastructure projects represented by EMBL
 - System biology at EMBL requires a collaborative, scalable and secure IT environment to enable research and to protect Intellectual Property
 - The understanding of the security in the data field focuses on the Identity and Access management for a growing impressive number of distributed users

- and data (across 5 sites)
- The introduced identity management and provisioning infrastructure is one key component to support the requirement for fine-tuning individual access scenarios
- The basic approach rely on Service Oriented Architecture (Web Services, Database Federation, Grid Approach)
- Identity and Access management based on LDAP, unified Login and SSO

Following recommendations can be outlined:

- Identify and address the incompatible approaches in Access Management which characterize the NREN and Grid domains, with the goal to reach a convergent solution.
- There exists a well-established CERT collaboration in the NREN-community. This platform can easily accommodate the needs of other communities. The adoption of the CERT collaboration model by other domains should be envisaged. That would avoid the need of replicating the service.
- The data community should organise itself to a sufficient degree to be able to establish a common understanding regarding security issues that covers all major data-related activities. The potential synergies offered by a coherent model for data security should be exploited. The cooperation with established domains will allow the sharing of their know-how and implemented services.

Cyberinfrastructures and e-Infrastructure initiatives.

While providing access to distributed resources controlled by different institutions, e-Infrastructures (US: cyber infrastructures) are a key component for collaborative research and innovation. For achieving such high level goals, development of public policies and incentives for advancing knowledge across institutional boundaries on a global perspective are essential. Three initiatives originating from large geographical areas (Japan, USA and Europe) and relying on different perspectives have been presented in the second session. Kento Aida from the National Institute of Informatics of Japan (NII) gave an overview of Cyber Science Infrastructure (CSI). CSI is a new information infrastructure to boost today's advanced scientific research in Japan including networking, federated ID management and grids. Bill Feiereisen from the American National Science Center outlined the impact of recent advances in HPC computing and the future opportunities enabled by the field. He emphasized the need for stronger collaboration between the US and Europe in e-Infrastructure development efforts. Kyriakos Baxevanides, Deputy Head of the Research Infrastructures Unit of the European Commission, presented the e-Infrastructure projects and efforts of the international collaboration efforts between e-Infrastructures during the European Commission's 7th Framework Program. He also accentuated the role of the European Union in supporting the development of global cross-disciplinary research infrastructures in the future.

Findings and recommendations

- Initiate a program, steered by the e-IRG, between the US and the EU to foster the collaboration in the field of the e-Infrastructure development.

Virtualization: A new trend and its impact on research e-infrastructures.

The aim of this session was to address the new trends and to envision the possible impacts of virtualization on the research e-Infrastructure and its applications. Grid computing, cloud computing, utility computing are just few of the technological and service concepts that are optimally positioned to benefit from new virtualization tech-

nologies and tools. As a concept, virtualization has many interpretations and implementations. The presentations, two from major commercial e-Infrastructure providers and one from a major forward-looking academic research project funded by the European Commission, illustrated different aspects of the concept and its applications. The fact that the major commercial information and services providers are heavily investing in this technology demonstrates a clear trend, which to date has not been tackled by research and education communities.

Findings and recommendations

- Include the aspects of virtualization and related implementations trends in the White Paper in order to assess the interest and possible applications for the research and education communities, particularly related to the flagship projects funded by the European Commission.

A closed meeting of the e-IRG delegates followed the workshop. Leif Laaksonen, Chair of the e-IRG, stated immediately after the meeting that securing the information infrastructure to create confidence among the key stakeholders will be a major challenge for the e-IRG.

The e-IRG Workshop program and presented material is available at:
http://www.e-irg.eu/index.php?option=com_content&task=view&id=54&Itemid=8