SEVENTH FRAMEWORK PROGRAMME

Inventory of existing PA-RIs cooperation – Update

FP7-ICT-248295/INFN/R/PU/D3.2 – PART II

Project Number:	FP7-ICT-2007-4 248295
Project Title:	Towards an Open and Sustainable ICT Research Infrastructure Strategy (OSIRIS)

Contractual Date of Deliverable:	30/11/2011 (month 23)
Actual Date of Delivery:	**30/11/2011**
Workpackage contributing to the Deliverable:	WP3 : Benchmarking
Nature of the Deliverable	R
Dissemination level of Deliverable	PU

Authors: INFN / Antonio Candiello, Mirco Mazzucato

Contributors:
NCF / Rossend Llurba [PRACE, SURFnet NREN, NCF HPC, BigGrid NGI, CSC HPC]
CESNET / Helmut Sverenyák [GÉANT, CESNET NREN]
CSEM / Arno Hoogerwerf [MNTEurope, MNT HTA]
IBBT / Rosette Vandenbroucke [Begrid NGI, Belnet NREN, DC.NET, Sunet NREN]
IBBT / Piet Demeester [Epixnet, FIRE],
IMEC / Cor Claeys [Sinano, IMEC Centre]
INFN / Alessandra Casotto [IGI NREN, EGI, EMI],
INFN / Marco Verlato [GMES/Cyclops, VRC NMR],
INFN / Marco Paganoni [VRC WLCG]
TNI-UCC / Cian O'Murchu [Tyndal NAP]
External contributors / Cal Loomis [Stratuslab]
External contributors / Andrea Manieri [Venus-C]
External contributors / Laurent Romary [Dariah]
External contributors / Saverio Vicario [Lifewatch IT]
External contributors / Milan Prica [Instrument Element]
External contributors / Damien Lecarpentier [EUDAT]

Reviewed by: TNI-UCC / Alan Mathewson, Cian O'Murchu
CSIR / Colin Wright

Abstract:

This deliverable will list the most relevant cases of current cooperation between Public Authorities and ICT Research Infrastructures. This will include a standardized and structured high-level list of relevant ICT Research Infrastructures, which identifies the appropriate network RIs, computing RIs, Micro & Nano Technologies (MNT) and instrumental-related infrastructures, data infrastructures and Future Internet.

Keyword list:
Research Infrastructures, ICT, inventory, cooperation.

Clarification

Nature of the Deliverable

R Report
P Prototype
D Demonstrator
O Other

Dissemination level of Deliverable:

PU Public
PP Restricted to other programme participants (including the Commission Services)
RE Restricted to a group specified by the consortium (including the Commission Services)
CO Confidential, only for members of the consortium (including the Commission Services)

Disclaimer

The information, documentation and figures available in this deliverable, are written by the OSIRIS ("Towards an Open and Sustainable ICT Research Infrastructure Strategy"*) – project consortium under EC co-financing contract FP7-ICT-248295 and does not necessarily reflect the views of the European Commission.*

Executive summary

This document lists the most relevant cases of current cooperation between *Public Authorities* (PA) and *National Champions* (NC) within existing ICT *Research Infrastructures* (RIs) for the requirements of the Osiris project.

A high-level list of relevant ICT Research Infrastructure models is reported, which identifies the relevant network RIs, computing RIs, *Micro & Nano Technologies* (MNT) and instrumental-related infrastructures, digital libraries frameworks. The Future Internet vision was also considered in this inventory.

The domains have been identified on the basis of several publications, including "The Future of Internet, Report from the National ICT Research Directors WGFI" [WGFI, 2008], "e-IRG Report on Data Management [DMTF, 2009], "Riding the wave – How Europe can gain from the rising tide of scientific data" [HlEGSD, 2010], "Trends in European Research Infrastructures Analysis of data from the 2006/07 survey", [EC-ESF, 2007], "EGI Blueprint" [EGI_DS, 2008], and the recommendations by consortium members and the stakeholder group.

For each domain, the relevant projects, the governance models and challenges experienced have been analysed. The consortium members provided the required input in order to better evaluate the cases of PA/NC cooperation within ICT RIs. A detailed list of intra-domain PA/NC-RIs collaborations is also reported.

This inventory will serve as a basis for the planned subsequent benchmark analysis.

Content

Inventory of PA/NC-RIs Collaborations

In order to better investigate the collaborations, the project selected a subset of the collaboration models within each RI domain for deeper scrutiny. The selected cases were enumerated with a (C#) code and assigned to an individual project partner. For this survey we followed a *common template*:

a) Description of RI
External contributors were asked to report a clear description of the Research Infrastructure.

b) PA/NC collaboration explanation
External contributors were asked to explain the nature of cooperation involvement of Public Authorities and/or "National Champions", aimed at identifying the best practice cases and methodologies as the basis for the development of models and suggestions for future RIs.

c) Budget, funding model, economic sustainability
External contributors were asked to report the budget of the PA/NC RI collaboration – both initial and recurrent investments – the running cost, the funding model and economic sustainability of the RI.

d) Governance / Management
External contributors were asked to describe the governance bodies, their relations and the management model.

e) Users and interaction model
External contributors were asked to specify quantitative and qualitative aspects regarding RI users – how many, from where, how they use the facilities and how they obtain access.

f) Countries and international collaborations
External contributors were asked to specify the countries involved and the international collaboration within and outside Europe.

g) History and evolution
External contributors were asked to outline the RI evolution from the first experiences to the current model, cite relevant previous projects/collaborations.

h) Security
External contributors were asked to specify privacy, protocols, trust, procedures and property rights for the RI.

i) Operations
External contributors were asked to report on the activities needed and the related efforts

The template-based survey was then assigned to OSIRIS project partners for submission to (internal or) external contributors.

The selected cases are shown in the following table:

Cod.	PA/NC Research Infrastructure Case	Assigned	Received	Contributor
(C01)	SURFnet: Dutch NREN	NCF	15/05/2011	Rossend Llurba
(C02)	Belnet: Belgian NREN	IBBT	16/03/2011	Rosette Vanderbroucke
(C03)	SUNET: Swedish NREN	IBBT	18/05/2011	Rosette Vanderbroucke
(C04)	CESNET: Czech NREN	CESNET	20/05/2011	Helmut Sverenyák
(C05)	GÉANT Project Collaboration	CESNET	06/04/2011	Helmut Sverenyák
(C06)	IGI: Italian NGI	INFN	25/02/2011	Alessandra Casotto
(C07)	BEgrid: Belgian NGI	IBBT	27/02/2011	Rosette Vanderbroucke
(C08)	BiG Grid: Dutch NGI	NCF	15/05/2011	Rossend Llurba
(C09)	EGI.eu Organization and EGI-InSPIRE Project collaborations	INFN	25/02/2011	Antonio Candiello
(C10)	The EMI Grid Mware Provider collaboration	INFN	03/03/2011	Alessandra Casotto
(C11)	The StratusLab OS Cloud Middleware Provider Collaboration	INFN	13/03/2011	Cal Loomis
(C12)	The Venus-C Public/Private Cloud M.Ware Provider Collaboration	INFN	25/03/2011	Andrea Manieri
(C13)	The WLCG HEP Physics VRC	INFN	01/04/2011	Marco Paganoni
(C14)	The WeNMR VRC	INFN	03/03/2011	Marco Verlato
(C15)	The Netherlands Computing Facilities Foundation (NCF)	NCF	15/05/2011	Rossend Llurba
(C16)	The CSC Finland HPC Centre	NCF	15/05/2011	Rossend Llurba
(C17)	The PRACE/DEISA HPC Centres Collaboration	NCF	06/04/2011	Rossend Llurba
(C18)	The Irish Tyndall National Research Centre	TNI-UCC	25/02/2011	Cian O'Murchu
(C19)	The Belgian IMEC National Research Centre	IMEC	15/03/2011	Cor Claeys
(C20)	The Epixnet Network of Excellence	IBBT	11/03/2011	Piet Demeester
(C21)	The MNT Europe Project Collaboration	CSEM	24/02/2011	Arno Hoogerwerf
(C22)	The Sinano Institute Collaboration	IMEC	15/03/2011	Cor Claeys
(C23)	The MNT Heterogeneous Technology Alliance (HTA)	CSEM	24/02/2011	Arno Hoogerwerf
(C24)	The Open Access Infrastructure for Research in Europe (OpenAIRE)	INFN	21/03/2011	Antonio Candiello
(C25)	The EUDAT (EUropean DATa) Project	INFN	28/02/2011	Damien Lecarpentier
(C26)	The Digital Cultural Heritage Network DC.NET	IBBT	27/02/2011	Rosette Vanderbroucke
(C27)	DARIAH ESFRI	INFN	18/03/2011	Laurent Romary
(C28)	Lifewatch – Italian National Network	INFN	18/03/2011	Saverio Vicario
(C29)	The Instrument Element (IE) Infrastructure Access Model	INFN	11/03/2011	Milan Prica
(C30)	The Global Monitoring Access Model (Cyclops)	INFN	03/03/2011	Marco Verlato
(C31)	The FP7 FIRE Initiative	IBBT	13/03/2011	Piet Demeester

The cases are representative of the following RI classes of collaboration models:

- **ICT National Initiatives** (NRENs, NGIs, HPC National Centres, MNT National Centres / Initiatives):
  C01-04 (NRENs), C06-08 (NGIs), C15-16 (HPC NCs), C18-19 (MNT NCs/NIs);
- **European ICT RIs and Collaborations**:
  C05 (GÉANT), C09 (EGI), C17 (PRACE), C20-23 (MNT inter-centre collaborations), C24-25 (OpenAIRE & EUDAT);
- **(ICT RI) R&D-related Projects**:
  C10-12 (DCI middleware), C29-30 (IE/GMES), C31 (FIRE);
- **Domain-related Community Networks**:
  C13-14 (VRCs), C26-28 (ESFRI-related).

We report the selected cases in the following sections.

1. The European and National Network RI environment

1.1 National Research & Education Networks (NRENs) Collaboration

(C1) SURFnet: Dutch NREN

Web Site / Document repository / Wiki: www.surfnet.nl

Contractual documents:

Contact person: Kees Neggers (Director)

1a) Description of RI

SURFnet is the *National Research and Education Network* (NREN) in the Netherlands. SURFnet provides internet connectivity and services to Dutch higher education institutes, research organisations, university hospitals and libraries.

SURFnet promotes, develops and operates a hybrid end-to-end fibre network. Institutes can connect to the Internet at 1 or 10 Gbps. IPv6 and multicast protocols are supported. SURFnet also provides direct connections between two locations through lightpaths (fixed and dynamic). Optical private networks are also provided, e.g. between the three technical universities in the Netherlands or between geographically different sites of one higher education institute. SURFnet has set up the *Netherlight GLIF Open Lightpath Exchange* to allow for international lightpath connections.

SURFnet provides trusted identity services (SURFfederatie).

1b) PA/NC collaboration explanation

SURFnet is a non-profit foundation which is owned by the SURF Foundation, the Dutch higher education and research partnership for ICT-driven innovation in which all Dutch

universities and research centres collaborate. SURFnet, however, is an autonomous legal entity and has its own management, staff and budget.

1c) Budget, funding model, economic sustainability

The budget of SURFnet was € 34.6 million in 2010. 64.1% was provided by charging connected organisations for the services provided, 32.6% was funded by public authorities and 3.3% by EU grants for FP7 projects. Approximately 40% of the budget is used for staff salaries and office costs, 20% for equipment and 40% for transmission capacity.

The connected organisations pay a flat fee (depending on the connection bandwidth and the number of users). Some services are charged separately (e.g. lightpaths). SURFnet has long term agreements for these fees which contribute to the sustainability of the funding model.

1d) Governance / Management

SURFnet is owned by the SURF Foundation whose shareholders (the Dutch higher education institutes, research organisations and libraries) appoint a Board of Directors for SURFnet. The management of SURFnet consists of two managing directors, a CTO and a CFO.

1e) Users and interaction model

In 2010, 14 universities, 64 higher education institutes, 32 research institutes, 19 libraries and 11 hospitals were connected to SURFnet. All connected institutes have a contact person for liaison with SURFnet. A user panel provides feedback on the services and the innovation plans. Theme oriented workshops and seminars are organised regularly and every two years a two-day conference is held.

1f) Countries and international collaborations

SURFnet has direct connections to GÉANT, Starlight and MANLAN, the commercial internet (TINET and TATA) and AMS-IX, the *Amsterdam Internet Exchange*. Cross border fibres to Hamburg, Aachen, Münster and Geneva are operational. SURFnet participates in the international collaborations TERENA, DANTE, GLIF and GLORIAD.

1g) History and evolution

SURFnet began in 1988 as a joint company of SURF Foundation (51% shares) and KPN, the Dutch telecom provider at that time, (49% shares). KPN sold its shares in 2001 to SURF Foundation. The first network (SURFnet1) was based on 64 Kbps connections. SURFnet6, today's operational network, is fully dark fibre based (11500 km), has 308 PoPs, and has a backbone capacity of 20 Gbps. SURFnet6, operational in 2006 was the world's first nation-wide hybrid network providing IP connectivity and lightpaths. In 2009 the GigaPort3 project started to create SURFnet7 which will deploy Next Generation Ethernet technology.

1h) Security

SURFnet has implemented all security measures and features that are common when operating a national network.

1i) Operations

SURFnet has a staff of 76.5 FTE and employs 57 FTE from subcontractors (16 for the NOC and 38 for other technical and user support).

(C2) Belnet: Belgian NREN

Web Site: www.belnet.be

Contractual documents:

Contact person: Pierre Bruyère, Director

2a) Description of RI

Belnet is the Belgian national research network that provides high-bandwidth internet connection and services to Belgian universities, colleges, schools, research centres, and government departments. Today, the organisation operates a full optical fibre network with connections of 10 Gbps and more, offering virtually unlimited bandwidth. Belnet also provides internet access with a very high bandwidth.

For the benefit of internet service and content providers and large private companies, Belnet operates a central infrastructure for exchanging internet traffic, called the Belgian National Internet Exchange or BNIX. Other activities are the *Federal Metropolitan Area Network* (FedMAN), the computing network GRID (BEgrid) and the Belgian National Computer Emergency Response Team, CERT.be.

CERT.BE takes Belnet beyond the boundaries of education and research by providing a service for every citizen in the country.

2b) PA/NC collaboration explanation

Belnet is a state service with independent management, managing its own budget and personnel.

2c) Budget, funding model, economic sustainability

Belnet is funded partially by a grant from the federal government and partially by its services offering. According to the 2009 yearly report the budget for that year amounted to € 12,029,821, of which € 8,474,000 accrued from the grant and the remainder from its own income.

This funding model has proven sustainable.

2d) Governance / Management

Belnet is led by its director who is assisted by a management committee. Members of the management committee belong to the federal government, to universities or to research organizations.

2e) Users and interaction model

In 2009 Belnet counted 193 customers and 700,374 end users. The customers are universities, colleges, public and private research centres, federal scientific institutions and a number of government institutions, some federal, regional and local administrations. All these customers have a contractual relation with Belnet whilst the end users use the network and its basic services in a transparent way. Belnet stays continuously in contact with its customers by means of the customer relations team that listens to the customer requirements. Regularly Belnet carries out a large scale customer satisfaction survey. Contact with end users is realized via conferences and workshops.

2f) Countries and international collaborations

Belnet works internationally with DANTE, which coordinates GÉANT2, the European Research Network; with Euro-IX the European Internet Exchange Portal, and with TERENA, the Trans-European Research and Education Networking Association.

2g) History and evolution

Belnet started in 1993 as an operational unit within the Federal Science Policy Office, serving 24 customers by providing interconnection between them at 64 Kbps. In the ensuing 17 years Belnet has evolved into a state service with independent management and serves 193 customers (700,374 end users). Over the years Belnet has added two other networks to the Belnet network: BNIX for Internet traffic between Belgian Internet providers and FEDMAN for internal traffic between federal administrations as well as their Internet traffic. The Belnet network is state of the art and is fully comparable with the largest research networks in Europe. With such an infrastructure Belnet was able to change its focus from infrastructure to providing specific services for higher education and research.

2h) Security

All usual security measures for network are in place.

2i) Operations

To manage the network and deliver all its services Belnet employs a staff of about forty *Full Time Equivalents* (FTE). Moreover, in order to guarantee 24x7 service monitoring and first level helpdesk are outsourced.

(C3) SUNET: Swedish NREN

Web Site / Document repository / Wiki: www.sunet.se

Contractual documents:

Contact person:

3a) Description of RI

SUNET (*Swedish University Computer Network*) provides high-speed Internet access to academic institutions in Sweden. The current incarnation of the network, OptoSunet, provides dual 10 Gbps links to each of the larger universities. SUNET's upstream network is the Nordic NORDUnet.

SUNET is dedicated to support the needs of the research and education communities within Sweden. The aim for SUNET is to provide Swedish universities and colleges with access to well-developed and functioning national and international data communication and related services, sufficient for their needs – regardless of their geographical location.

Apart from offering high-capacity computer networks, SUNET also provides a variety of different services for connected organizations. The services of SUNET are partly government funded and partly funded by charges to connected organizations.

SUNET supports several high-demand eScience projects; SUNET is a vital part of the Swedish Research Infrastructure.

3b) PA/NC collaboration explanation

3c) Budget, funding model, economic sustainability

SUNET is a specialized Internet service provider dedicated to supporting the needs of the research and education communities within Sweden. Connection to the OptoSunet network is limited to research and education communities within Sweden and to organizations in Sweden co-operating with research and education communities. The budget for SUNET is approximately €17,100,000 per year, of which approximately €4,500,000 is a yearly governmental grant. Refer to the TERENA Compendium for details of the SUNET network.

3d) Governance / Management

The Swedish Research Council, which is administratively responsible for SUNET, is an authority inside the Department of Education and Culture, and is the largest Swedish funding agency for basic research at Swedish universities, colleges and institutes.

SUNET and the other research networks in the Nordic countries use NORDUnet for joint communication with the rest of the world. As a member of NORDUnet, SUNET is also connected to GÉANT, the European research network.

3e) Users and interaction model

All personnel, students, researchers etc. at all universities and university colleges in Sweden have access to SUNET through their university LAN. Access is also provided to other organizations with close relationship with the research and education community. In total, there are of the order of 450,000-500,000 students and approx. 100,000 other users using the network. The TERENA Compendium contains further details of the network.

3f) Countries and international collaborations

SUNET and the other research networks in the Nordic countries use NORDUnet for joint communication with the rest of the world. As a member of NORDUnet, SUNET is also connected to GÉANT, the European research network.

3g) History and evolution

SUNET started in the mid-1980s as a research project for Swedish computer scientists, and paved the road for Internet in Sweden. SUNET is governed by a board appointed by the Swedish research council. In addition to the board there is a technical reference group, as well as people working at the participating universities.

3h) Security

SUNET forwards all traffic between connected parties. No filtering etc. is carried out, as that is up to each organization. Traffic protocol is IP. Refer to the TERENA Compendium for details.

3i) Operations

(C4) CESNET: Czech NREN

Web Site / Document repository / Wiki: www.ces.net

Contractual documents: Association Foundation Agreement, Statutes

Contact person: Jan Gruntorád, CEO

4a) Description of RI

CESNET, z.s.p.o., association of legal entities, was founded in 1996 by all universities of the Czech Republic and the Czech Academy of Sciences.

The CESNET provides and develops two e-infrastructures for the Czech academic community:

- *high-speed computer network* for the science, research, development and education purposes – *CESNET2*. The backbone network interconnects the largest university cities of the Czech Republic with circuits featuring high transfer rates (10 Gbps). Users of the network include first of all universities and the Academy of Sciences of the Czech Republic as well as several high schools, hospitals, or libraries.
- *National Grid Infrastructure – MetaCentrum*. MetaCentrum operates and manages distributed computing infrastructure consisting of computing and storage resources owned by CESNET as well as those of co-operative academic centres within the Czech Republic. MetaCentrum is responsible for building the National Grid and its integration to related international activities, especially in the European Union. MetaCentrum performs a variety of *coordinating functions*, including central authentication and authorization, management of virtual organizations, distribution and scheduling of compute jobs, maintenance and monitoring of resources and consulting services and support of scientific communities.

In addition to the infrastructures mentioned above, the CESNET also offers to its users some advanced services including AAI infrastructures and collaborative tools.

4b) PA/NC collaboration explanation

CESNET is an association of Czech public universities and the Academy of Sciences of the Czech Republic. These institutions are very dependent on both infrastructures and their services. CESNET has a close relationship with the Ministry of Education, Youth and Sports which provides a significant public subsidy for CESNET's activities (see section c). In 2009, CESNET was been appointed as a National Grid Initiative by the Ministry of Education, Youth and Sports of the Czech Republic.

In 2010 the Czech Government approved CESNET's infrastructure as a Large Infrastructure for Research and Development and approved public support of the project called "Large infrastructure CESNET, the part of European GÉANT and EGI" for the period 2011 – 2015. CESNET became a part of the National Roadmap of Infrastructures for Research, Development and Innovations.

4c) Budget, funding model, economic sustainability

The CESNET Association performs its activities within the scope of the subsidies gained and partial compensation of expenses related to these activities. The Association's objective is not to generate any profit. In addition to its main activities, the Association also pursues economic/business activities; however, solely for the purpose of making more efficient use of its property and without any negative impact on research activities.

Current annual budget is about 16 million Euro and the income accrues from the following sources:

Users / Clients	25 %
Government / Public Bodies	70 %
The EU (e.g. for Framework Program projects)	5 %

The public funding for years 2011 – 2015 is ensured within the subsidy of project "Large infrastructure CESNET, the part of European GÉANT and EGI" (LM2010005).

Besides the resources mentioned above, the subsidy for the upgrade and extension of the regional infrastructures (namely for the purpose of ensuring connectivity and advanced ICT services for emerging research infrastructures) of about 24 million Euro over the period May 2011 – October 2013 has been assigned by the Ministry of Youth, Education and Sport of the Czech Republic within the ESF Operational Program "Research and Development for Innovations" framework.

4d) Governance / Management

CESNET is an association of Czech public universities and the Academy of Sciences of the Czech Republic. The list of members follows:

1. Charles University, Praha
2. Palacky University, Olomouc
3. Czech Technical University, Praha
4. Technical University of Ostrava
5. Academy of Arts, Architecture and Design, Praha

6. Academy of Fine Arts, Praha
7. Brno University of Technology
8. University of Veterinary and Pharmaceutical Sciences, Brno
9. Masaryk University, Brno
10. Mendel University of Agriculture and Forestry, Brno
11. Academy of Performing Arts, Praha
12. Janacek Academy of Music and Dramatic Arts, Brno
13. University of Pardubice
14. Institute of Chemical Technology, Praha
15. Czech University of Agriculture in Prague
16. Technical University of Liberec
17. University of Economics in Prague
18. University of Hradec Kralove
19. University of South Bohemia, Ceske Budejovice
20. University of Ostrava
21. Silesian University, Opava
22. Jan Evangelista Purkyne University in Usti nad Labem
23. University of West Bohemia, Plzen
24. University of Defence, Brno
25. The Academy of Sciences of the Czech Republic
26. Tomas Baťa University, Zlín

The *General Assembly*, which is the highest authority of CESNET, is held twice per year, usually in July and December. The statutory authority, termed the *Board of Directors*, consists of seven members and provides strategic management and acts on CESNET's behalf. A five member *Advisory Board* advises the Board of Directors and management of CESNET. The day-to-day operational management is performed by the *Chief Executive Officer*.

The CESNET staff consists of about 200 employees, representing 130 FTEs. The internal structure as follows:

- Department of External Relations,
- Department of Information System,
- Financial Department,
- Legal Department;

Research, Development and Innovation *Section* divided into following departments:

- Network Development,
- Grids,
- Data Storages,
- Multimedia,
- Optical Networks,
- Technologies for Network Applications,
- Monitoring and Configuration Tools,
- Support Services and CSIRT,
- Network Identity,
- Service Desk,
- Support of R&D.

4e) Users and interaction model

Infrastructure services are not provided to the public. Users of the infrastructure include first of all universities and the Academy of Sciences of the Czech Republic, nevertheless other organisations meeting the Access Policy[1], such as institutions providing R&D activities, high schools, hospitals, or libraries are allowed.

CESNET pays great attention to search for and support applications requiring above-standard communication with high demands for data transfer parameters (such as unusual volume, transfer rate, response time or reliability) and/or requiring special transfer modes that cannot be achieved in a shared IP network. For these applications, end-to-end routes and private and virtual networks at various levels are created, ensuring the required parameters and the transfer quality needed.

The most important and long-term supported community is that of *High Energy Physics* (HEP)**.**

The particle physics community in the Czech Republic is actively involved in the LHC TEVATRON and RHIC accelerator experiments, as well as in astrophysics experiments. For this community CESNET provides access to network resources in the following two ways:

- high-speed access to IP services (both IPv4 and IPv6), and
- dedicated international high performance lines (so called end-to-end or lambda services).

Support of research grids-a- large (but primarily for HEP) is a subject of the EGI (European Grid Initiative) and its supported international projects, in which CESNET is actively involved as the National Grid Initiative.

The most important HEP groups in the Czech Republic are:

1. Institute of Physics, ASCR, Prague,
2. Nuclear Physics Institute, ASCR, Řež,
3. Faculty of Mathematics and Physics, Charles University, Prague,
4. Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University, Prague,
5. Institute of Experimental and Applied Physics, Czech Technical University, Prague.

In addition to standard IP connectivity, these institutes are connected to the CESNET2 node located in CESNET's premises in Prague using 1 or 10 GE lambdas.

The Institute of Physics hosts the Regional Computing Centre for Particle Physics that serves, together with CESNET's grid computing centre, as a distributed Tier2 centre of the *LHC Computing Grid* (LCG) project. Its main computing resources (20 kHEPSPEC2006 and 450 TB in 2010) are devoted to the D0 experiment at the Tevatron Run2, the STAR experiment at RHIC, astrophysics AUGER experiment as well as the ATLAS and ALICE LHC

[1] See: http://www.ces.net/doc/aup.html.

experiments. The support given to LHC experiments will soon dominate the usage of resources. For this Tier2 centre CESNET has established following lambdas:

- within the GÉANT+ service and with the co-operation of the German NREN DFN, a circuit at the capacity of 1 Gbps to the Tier2 Centre in Karlsruhe,
- a link from Prague to Fermilab. This link is used intensively for the D0 experiment data processing at the Prague Regional Centre,
- a link from Prague to BNL. The link is used by the STAR experiment and later for connection to the BNL's ATLAS Tier1 centre.

A link between Prague and Taipei interconnects the Tier2 Regional Computing Centre for Particle Physics with the Tier1 centre in Taiwan's Academia Sinica Grid Computing Centre.

VO Auger

The VO (Virtual Organisation) Auger was setup for members of the Pierre Auger collaboration. The *Pierre Auger Cosmic Ray Observatory* is studying ultra-high energy cosmic rays, the most energetic and rarest of particles in the universe. When these particles strike the earth's atmosphere, they produce extensive air showers made of billions of secondary particles.

Computing resources provided for Auger VO will be either dedicated resources of groups taking part in the collaboration or "opportunistic" resources of other organizations offered on a voluntary basis. Resources for the VO infrastructure (registration server, voms and ldap server) are provided by CESNET (within EGI) and by the Institute of Physics of the Academy of Sciences of the Czech Republic.[2]

Support of other research communities.

Very interesting area from ICT point of view are medical applications dealing with graphic data collected with modern scanning devices in hospitals (X-ray, MRI, CT) and applications from the field of physics processing data created in unique devices (electron microscopes, radiation detectors etc.). Data transfers connected with real-time 3D image modelling, virtual reality and high-resolution video are becoming more and more frequent in network applications.

CESNET also started a co-operation with both current and emerging research infrastructures in Czech Republic:

- BIOCEV – www.biocev.eu/en.html,
- CEITEC – www.ceitec.eu,
- CESSDA – www.cessda.org,
- CLARIN – www.clarin.eu,
- ELIXIR – www.elixir-europe.org,
- INFRAFRONTIER – www.infrafrontier.eu,

[2] More information and access rules are on www.metacentrum.cz/en/VO/auger/index.html.

- IT4INNOVATIONS (will be part of PRACE) – www.it4i.eu.

4f) Countries and international collaborations

The CESNET Association is a member of important international and national organizations including:

- TERENA (*Trans-European Research and Education Network Association*) – established in 1994 through the merger of EARN (*European Academic and Research Network*) and RARE (*Réseaux Associés pour la Recherche Européenne*). It is engaged in the development of the telecommunication infrastructure of academic and scientific sites across Europe.
- CEENet (*Central and Eastern European Networking Association*) – organization coordinating international telecommunication activities of countries in Central and Eastern Europe.
- GLIF (*Global Lambda Integrated Facility*) – global experimental network activities, focusing on the development support for most demanding scientific and research applications. The main goal of this project is to construct a network that will service applications with extreme transfer rate requirements.
- DANTE (*Delivery of Advanced Network Technology to Europe* Ltd.) – a non-profit organization aimed at the construction and quality improvement of IP connectivity for academic institutions in European countries.
- Internet2 – consortium led by American research and education institutions which endeavours to develop and deploy new types of network technologies, services and applications. The CESNET Association has been an associate member of the consortium since 1999.
- PlanetLab – consortium of academic, commercial and governmental organizations from the entire world, collectively operating a global computer network designed for developing and testing new telecommunication applications. There are currently 780 nodes from 31 countries operating in the network.
- EGI.eu – organization focusing on coordination of European computing grids used for scientific calculations and their sustainable development support.
- NIX.CZ – CESNET is one of the founders of NIX.CZ. (*Neutral Internet Exchange*), an association of Internet service providers in the Czech Republic, offering the possibility of mutual interconnection of member networks.
- CZ.NIC – CESNET is also one of the founding members of CZ.NIC an organization engaged in the domain registration, support of projects of general benefit and Internet-related activities.

Since the founding of CESNET, it has participated in a variety of projects requiring international collaboration namely in the area of building both European communication (GÉANT) and grid (EGI) infrastructures. Recently, CESNET took part in the following set of projecst:

- GÉANT – www.geant.net,

- EGI-INSPIRE – www.egi.eu/projects/egi-inspire,
- EMI – www.eu-emi.eu,
- CHAIN – www.chain-project.eu.

4g) History and evolution

The Association was founded in 1996 by all the public universities in the Czech Republic, together with the Academy of Sciences of the Czech Republic (AV ČR). In 1996, when the Association received a grant for the TEN-34 CZ Network Deployment project from the Ministry of Youth, Education and Sport of the Czech Republic, the Association commenced building the academic backbone network at an entirely new level of quality. Simultaneously, academic and commercial traffic were separated and all CESNET members converted to the academic network.

From 1997, the Association operated two independent networks. The first, TEN-34 CZ (later TEN-155 CZ), served the needs of science, research and education, to which members of the Association and some other institutions complying with the Acceptable Use Policy were connected. The second network, for historical reasons called CESNET, connected commercial customers. After the commercial network was sold in 2000, the Association ceased to act as a commercial Internet provider. Since then, it has engaged solely in the operation of the science, research and education backbone network (National Research and Education Network, NREN of the Czech Republic) and other related activities.

During the period 2004 to 2010, the Association obtained subsidies in the form of institutional support for its research plan, entitled Optical National Research Network and Its New Applications, the draft of which was submitted in 2003. In 2009 CESNET was appointed as a National Grid Initiative by the Ministry of Education, Youth and Sports of the Czech Republic.

In 2011, a new phase of national e-Infrastructure development started. The upgrade and reconstruction of communication and grid infrastructure as well as the building up of a national data storage infrastructure and development of NREN related services are within the framework of the five-year project: “Large infrastructure CESNET, the part of European GÉANT and EGI” (LM2010005) supported by Ministry of Education, Youth and Sports of the Czech Republic.

4h) Security

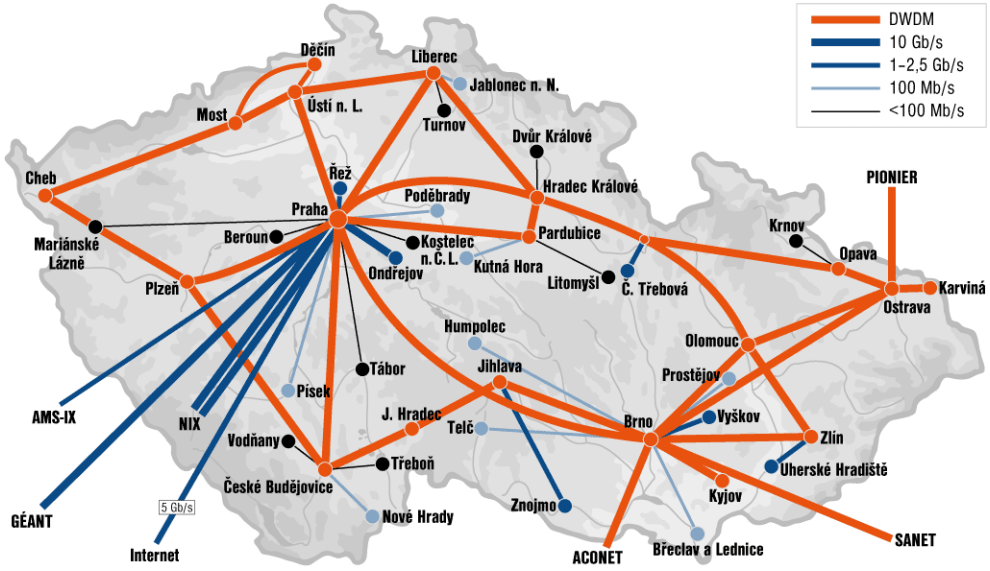
The aim of the CESNET CERTS activity is to achieve an enhanced internal organization in the area of security of the CESNET infrastructure and services that run on it. Preventive and active protection of computers and networks comprises consistent and efficient security incident handling, including addressing both their causes and consequences.

4i) Operations

The contemporary CESNET2 network is built around a DWDM core. It uses a mixture of commercial equipment and optical devices developed by CESNET. The remaining backbone lines of the CESNET2 network are based on a mixture of Ten-Gigabit and Gigabit Ethernet

and Packet Over SONET (POS). It ensures very high throughput (bandwidth of all core lines lies in the range of gigabits per second). The essential idea of network design is to build the backbone network in small rings encompassing no more than four cities (points of presence). Such topology provides redundant network offering small hop counts and delays.

Topology valid since March 2011



The network has the following independent international connections:

- 10 Gbps to GÉANT, used for academic traffic
- 2.5 Gbps to Telia, used for commodity traffic
- 10 Gbps to SANET, academic network of Slovakia
- 10 Gbps to ACOnet, academic network of Austria
- 10 Gbps to PIONIER, Polish optical academic network
- 10 Gbps to NetherLight/GLIF for experimental traffic; this line is connected to the experimental optical network, CzechLight, and is hence not depicted in the CESNET2 map above

In addition to these international lines, external connectivity of CESNET2 is enhanced by powerful peering connections:

- 2×10 Gbps to NIX.CZ,
- 1 Gbps to AMS-IX.

The network provides multicasting capability and is a part of the MBone network. IP version 6 is provided as a standard service.

The network is supervised by 365/7/24 Network Operating Centre.

A long-term goal of the MetaCentrum project is the operation and coordination of a distributed computing and data storage infrastructure in the Czech Republic as a dynamic network of resources across different locations and administrative domains, as a component of the pan-European infrastructure built on the framework of the EGI project, accompanied by

an appropriate support environment and continual expansion of available computational capacities. Currently MetaCentrum offers its users computational power comprising about1500 CPUs and storage capacity of about 400 TB.

Despite differences in hardware, operating systems and the physical location of computers, MetaCentrum's users have a common authentication trust domain, this implies one login and one password access to all machines involved in MetaCentrum.

1.2 Network Backbone (GÉANT) Project Collaboration

(C5) GÉANT Project Collaboration

Web Site: www.geant.net

Document repository: www.geant.net/Media_Centre/Media_Library/pages/home.aspx

Wiki:

Contractual documents: Grant agreement, Consortium Agreement

Contact person: Vasilis Maglaris, GÉANT NREN PC Chairman

5a) Description of RI

GÉANT is the high bandwidth pan-European research and education backbone that interconnects *National Research and Education Networks* (NRENs) across Europe and provides worldwide connectivity through links with other regional networks. The GÉANT network is a necessary communication environment for other Research Infrastructures in Europe. GÉANT provides:

- data transfer speeds of up to 10 Gbps, across 50,000 km of European network infrastructure, of which 12,000 km is based on own lit fibre,
- flexible, innovative architecture for data communications across the standard IP backbone, and for high capacity "private" network paths reserved for specific projects or disciplines,
- connectivity through European NRENs to an estimated *40 million* research and education *users* in over *8,000 campus networks* in *40 countries* across Europe.

5b) PA/NC collaboration explanation

The GÉANT project is a collaboration between 34 project partners: 36 European NRENs, DANTE and TERENA. Through the NREN partners, GÉANT delivers a range of services across the network for institutions, projects and researchers.

DANTE (www.dante.net) is the managing partner, project co-ordinator and operator of the GÉANT network. Established in 1993, DANTE has played a pivotal role in consecutive generations of the pan-European research network. The organisation also manages regional networking projects in Europe, Asia and the southern Mediterranean area.

TERENA (www.terena.org) handles a number of the outreach activities, and supports the co-ordination of the research and development effort amongst project partners. TERENA offers NRENs a forum in which to foster the development of Internet technology, infrastructure and services to be used by the research and education community.

NRENs: (National Research and Education Networks). Europe's NRENs are specialised Internet service providers dedicated to supporting the needs of the research and education communities within their own country.

5c) Budget, funding model, economic sustainability

The GÉANT network and associated programme of activities is co-funded by the European Commission within the GÉANT Project (GN3) contract, which is part of the EC's Seventh Research and Development Framework Programme. This contract between the project partners and the European Commission provides total funding from the EC of 93 million Euros for four years starting from 1 April 2009. Matching funding is provided by the NREN project partners connected to the network, the total budget being 182.18 million Euro.

5d) Governance / Management

The governance of such a large and complex infrastructure involves over 400 project participants based in organisations countries across the length and breadth of Europe. Close and streamlined collaboration is essential and structured communications for clear management vital in order to optimise performance and results and so ensure the success of the project.

Several bodies contribute to the overall successful running of the project through well-defined and well-organised management and control structures.

Policy Committee

The *Policy Committee* (often referred to as the NREN PC) consists of appointed representatives from each project partner. It meets at least three times a year, and is responsible for setting and overseeing overall policy. The Policy Committee Chairman is elected by the committee members for a two-year term and is currently Dr Vasilis Maglaris from *National Technical University of Athens* (NTUA).

Executive Committee

The *Executive Committee* is comprised of a small group elected by the Policy Committee. It is primarily responsible for preparing the yearly work programme for the project, and quality assurance and supervision related to its implementation. The committee includes a

number of non-voting members. These are individuals occupying the following posts within key research networking organisations:

- NREN PC Chair,
- DANTE Chair,
- DANTE General Managers,
- DANTE CFO,
- TERENA President,
- TERENA Secretary.

Project Management Team
The *Project Management Team* meets each month in order to discuss operational matters and is made up of following bodies:

- the day-to-day operational management of the project is performed by two *Project Managers* (DANTE General Managers) who are responsible for the coordination of the different Activities, supported by the Project Office;
- the *Project Office* looks after the project secretariat, financial and administrative responsibilities, as well as the five Coordination roles that ensure the synchronisation and coordination of efforts across all project Activities, and adherence to the project's technical and procedural guidelines and initiatives;
- the *Activity Leaders* are each responsible for a specific area of the project, across Research, Services and (human) Networking activities.

Project Coordinator
DANTE, Ltd as the coordinating partner provides overall project management and co-ordinates the project's various activities. It is responsible for financial and administrative work, including delivering progress reports to the EC. As the project co-ordinator, DANTE is also responsible for public relations, and for overall communications between the project and the EC.

5e) Users and interaction model

GÉANT provides Europe with a gateway for global collaboration, enabling researchers, students, teachers and other staff in institutions across the continent to participate in joint projects with their peers in other parts of the world. GÉANT offers different connectivity options and supporting network services to institutions, so enabling them to support the networking needs of their project and individuals.

As well as providing fast access to conventional web-based resources, GÉANT supports data-intensive and time-critical applications between collaborating partners throughout Europe and across the globe.

Through the co-operation and close collaboration of NRENs across Europe, and through links with other international networks, GÉANT enables researchers and projects to be more innovative, opening up new methods for research as well as new possibilities to share, exchange and process data and information.

European researchers in fields such as health and drug discovery, seismology and astronomy, crop research and weather forecasting are increasingly working more closely than ever before with their global counterparts, to address issues facing all corners of the world.

Many of these applications require distributed (grid) computing resources and can draw on the powerful grid projects (such as EGEE, DEISA and PRACE) which are enabled by the underlying network infrastructure.

Examples of user projects assisted by international research & education networks:

Particle Physics:

The *Large Hadron Collider* (LHC) is said to be the largest scientific endeavour in history. By colliding particles at extremely high energies, the LHC's experiments will generate some 15 Petabytes (15 million Gigabytes) of data annually. This huge amount of data is distributed to *eleven primary processing centres* around the world, from where it is accessed and analysed by thousands of scientists, engineers and support staff. GÉANT and the NREN partners have deployed a vast private network with sufficient bandwidth reserved specifically for LHC researchers to facilitate this data distribution and analysis, and linking each processing site to CERN by a dedicated connection. To support the *LHC Optical Private Network* (LHCOPN), GÉANT's perfSONAR multi-domain monitoring (MDM) service has been implemented to monitor network status and performance across each of these connections.

Radio Astronomy:

The EXPReS project uses dedicated high-speed GÉANT links to connect remote radio telescopes across Europe to a central data processor at JIVE, the *Joint Institute for Very Long Baseline Interferometry in Europe*, situated in the Netherlands. Here the enormous volumes of simultaneous observation data that are transmitted over the network are correlated to form very sharp, high-definition images of cosmic radio sources. Data was previously collected at each telescope on magnetic tapes and later onto hard disk. These physical media were transported by courier, taking several days. Now, information is sent from telescopes to the central computer in just seconds, enabling astronomers to create real-time views of the outer reaches of the universe.

Earth Observation - weather simulations for climate change researchers

The Millennium Simulations project by the Max Planck Institute for Meteorology, enables researchers into climate change to access simulations created by a major new Earth System Modelling initiative that spans the last millennium and forecasts into the future. The project uses the GÉANT network to connect remote research sites to its central system, helping to create a library of data and results which can be shared between project participants and the wider research community. The Earth System Model, created using climate data and models of natural external factors and man-made effects, allows scientists to simulate the climate from the last millennium and into the future. This research relies on employing many computer processors in parallel, which is only possible using the immense bandwidth capacity and geographical reach of the GÉANT network.

5f) Countries and international collaborations

The European NRENs involved in the GÉANT project are listed bellow:

ACOnet	www.aco.net	Austria
BASNET	www.bas-net.by	Belarus
BELnet	www.belnet.be	Belgium
BREN	www.bren.bg	Bulgaria
CARNet	www.carnet.hr	Croatia
CYNET	www.cynet.ac.cy	Cyprus
CESNET	www.ces.net	Czech Republic
EENet	www.eenet.ee	Estonia
RENATER	www.renater.fr	France
DFN	www.dfn.de	Germany
GRNET	www.grnet.gr	Greece
NIIF	www.niif.hu	Hungary
HEAnet	www.heanet.ie	Ireland
IUCC	www.iucc.ac.il	Israel
GARR	www.garr.net	Italy
SigmaNet	www.sigmanet.lv	Latvia
LITNET	www.litnet.lt	Lithuania
RESTENA	www.restena.lu	Luxembourg
MARNet	dns.marnet.net.mk	Macedonia
University of Malta	www.um.edu.mt	Malta
RENAM	www.renam.md	Moldova
MREN	www.mren.ac.me	Montenegro
SURFnet	www.surfnet.nl	Netherlands
NORDUnet	www.nordu.net	Nordic region (includes Norway, Sweden, Finland, Denmark and Iceland)
PSNC	www.man.poznan.pl	Poland
FCCN	www.fccn.pt	Portugal
AARNIEC/RoEduNet	www.nren.ro	Romania
JSCC	www.jscc.ru	Russia
AMRES	www.amres.ac.rs	Serbia
SANET	www.sanet.sk	Slovakia
ARNES	www.arnes.si	Slovenia
RedIris	www.rediris.es	Spain

SWITCH	www.switch.ch	Switzerland
ULAKBIM	www.ulakbim.gov.tr	Turkey
JANET	www.ja.net	UK
URAN	www.uran.net.ua	Ukraine

The global reach of the GÉANT network enables scientists and academics in Europe to exchange data and collaborate with their peers across the world through links to 59 National Research and Education Networks. With plans for regional research and education networks to be established in the Caribbean and Sub-Saharan Africa, GÉANT's global connectivity will continue to grow to reach all of the following regions:

North America:

The North American research networking environment is more diverse than in Europe, with research networking connectivity provided by CANARIE in Canada, and four main research and education networks in the USA: ESnet, Internet2, *National LambdaRail* (NLR) and the *NASA Integrated Services Network* (NISN).
There is a long–standing relationship between pan-European research networking and North American research networks. The connections to North America are key in enabling research collaboration on intercontinental projects, and are particularly significant for the *Large Hadron Collider* (LHC) at CERN, a number of the data-processing centres for which are located in North America.

Latin America:

The pan-Latin American research and education network, RedCLARA, currently interconnects 13 Latin American *National Research and Education Networks* (NRENs) and provides a 622-Mbps transatlantic link between Sao Paulo (Brazil) and Madrid (Spain) to the GÉANT network in Europe. RedCLARA is managed and operated by the RedCLARA non-profit organisation which was originally established in December 2004 as CLARA (*Latin American Cooperation of Advanced Networks*).

The RedCLARA network is partly funded by the European Commission through the ALICE2 project which is coordinated by the RedCLARA organisation. With 18 beneficiary countries in Latin America, ALICE2 is also partnered by four European NRENs (FCCN in Portugal, GARR in Italy, RENATER in France and RedIRIS in Spain) and DANTE.

North Africa and the Middle East:

EUMEDCONNECT2 is a high-capacity IP-based data-communications network which connects the research and education communities in seven countries (Algeria, Egypt, Tunisia, Jordan, Morocco, Palestian Territories and Syria) in the southern and eastern Mediterranean. via EUMEDCONNECT2 and GÉANT hubs. Offering direct links to GÉANT, EUMEDCONNECT2 connects approximately 2 million users in around 700 institutions across North Africa and the Middle East to collaborate with their peers in neighbouring countries and Europe. GÉANT is involved in finding networking solutions to facilitate concept of "multi-domain" networking services both across Europe and on a global scale.

Sub-Saharan Africa:

The UbuntuNet Alliance is a regional association of *National Research and Education Networks* (NRENs) in Africa. It was established in the latter half of 2005 by five established and emerging NRENs in Eastern and Southern Africa and now has a total of 13 NREN members (Democratic Republic of Congo, Ethiopia, Kenya, Malawi, Mozambique, Rwanda, Somalia, Sudan, South Africa, Tanzania, Uganda, Namibia, and Zambia).
The AfricaConnect contract between the EU, Ubuntunet and Dante was signed in May 2011. The EU majorly funded AfricaConnect will establish a high-capacity Internet network for research and education in Southern and Eastern Africa to provide the region with a gateway to global research collaboration. The initiative will dramatically accelerate the development of the Information Society in Africa, providing advanced data communications infrastructure and enabling African researchers to collaborate more easily in advanced international research projects. The AfricaConnect project is managed by Dante.

South Caucasus:

Co-funded by the European Union, the *Black Sea Interconnection* (BSI) ran from the spring of 2009 until late 2010 and provided connectivity for a regional network of the NRENs in Armenia (NASRA), Azerbaijan (AzRENA) and Georgia (GRENA) with an interconnection with GÉANT. The project was managed by ULAKBIM (Turkish NREN) with assistance from GRNET (Greek NREN), CEENet (*Central and Eastern European Networking Association*) and DANTE.

Central Asia:

The CAREN is a high-capacity regional research and education network in Central Asia (Kyrgzystan, Tajikistan, Turkmenistan, Kazachstan and Uzbekistan) to provide the region with a gateway to global research collaboration. Thanks to the interconnection with its pan-European counterpart GÉANT via the TEIN3 and ORIENT connections, CAREN allows researchers, educators and students across the region not only to collaborate with each other but also to engage in exciting joint projects with their peers in Europe and other parts of the world. The CAREN network became operational in the summer of 2010. Kazakhstan and Uzbekistan are expected to join the CAREN project in due course.

The NATO-led SILK Afghanistan initiative is a three-year project to provide high-speed interconnectivity between the GÉANT network and universities in Afghanistan. Connectivity is provided by the 43-Mbp satellite link to a teleport hub in Bratislava, from where traffic is carried via a terrestrial link to the GÉANT *Point of Presence* (PoP) in Vienna.

Asia-Pacific:

The third generation of the *Trans-Eurasia Information Network* (TEIN3) provides a dedicated high-capacity Internet network for research and education communities across Asia-Pacific. TEIN3 connects researchers and academics in China, India, Indonesia, Japan, Korea, Laos, Malaysia, Nepal, Pakistan, the Philippines, Singapore, Sri Lanka, Taiwan, Thailand, Vietnam and Australia. Bangladesh, Bhutan and Cambodia are in the process of being connected, bringing the total number of partners involved in TEIN3 to 19. With direct connectivity between the region and GÉANT via 2.5-Gbps links from Madrid to Mumbai and on to Singapore and also Copenhagen to Beijing via the ORIENT programme, TEIN3 offers the Asia-Pacific region a gateway for global collaboration, enabling over 45 million users at more

than 8,000 research and academic centres to participate in joint projects with their peers in Europe and other parts of the world.
The ORIENT link between Copenhagen and Beijing provides additional capacity of 2.5 Gbps between Europe and the Asia-Pacific region, offering a further peering point for GÉANT with the TEIN3 network, CERNET and CSTNET (*China Science and Technology Network*). The significant synergies between ORIENT and TEIN3 maximise bandwidth and reliability benefits to the user communities in Europe, Asia-Pacific and China. The ORIENT project's time-line was originally set between November 2005 and October 2008 and has been extended to the end of 2010. Plans for a successor project are being made.

5g) History and evolution

Since November 2000, when GÉANT was launched, it has dramatically increased its global reach. From just a handful of European countries connected in 2001, there are now high-speed links to nearly fifty countries outside of Europe and to international networks spanning the world. Working together, the combination of GÉANT, national research networks and international partners has created a truly global research community. Not only does this accelerate discoveries, new ideas and solutions, but it also enables researchers in less developed nations to collaborate and compete with peers throughout the world, bridging the digital divide and preventing, and even reversing, "brain drain".

In 2004 GÉANT became the first international 'hybrid' network, combining routed and switched infrastructure over 12,000 km of its own optical fibre. This enabled the creation of a portfolio of new services for users – from different speeds to dedicated, guaranteed high-capacity connections. By 2010, the range of users and their needs had become more diverse, encompassing humanities and science projects of all types and sizes, driven by three factors: viz increased openness to sharing information internationally, greater cross-disciplinary working and a centralized approach to information storage. With this growth has come a cultural shift with new challenges, beyond simply a need for high speed connections. There has developed an increased openness to sharing information internationally and a centralized approach to information storage with the challenge for researchers to ensure consistency of data structures, with user-friendly interfaces.

Ensuring that the power of the network is available to all, through simple, easy to use services is at the heart of GÉANT today and moving forwards. Created from user feedback, these services include advanced, end-to-end network monitoring that allows identification of problems before their impact is felt, secure roaming that enables researchers to work from anywhere within the network and, of course, the ability for users to easily control the speed and capacity necessary for their needs.

5h) Security

Security activities in GÉANT are in two categories:

- those intended to stop, mitigate and counteract intrusions and unwanted activities performed for malicious reasons. This is a mixture of reactive and proactive actions with the close cooperation of the NREN's Computer Security Incident Response Teams;

- those intended to ensure that services and resources are accessible only to those who have the correct rights of access. This is a mixture of enabling and protecting access and resources. The *eduroam* and *eduGAIN* infrastructures are results of such activities.

5i) Operations

To ensuring optimum performance across the GÉANT network, the Project Co-ordinator, DANTE, is responsible for the operation, management and development of the GÉANT network. The operation of the network incorporates two core tasks:

- *managing* the network *operation*,
- building the *network of tomorrow*.

5j) Operational Network Management

DANTE's operations department handles the co-ordination and execution of GÉANT's operational service provision. The department consists of the Operations Team, and the Network Operations Centre.

Operations Team

The operations team performs high level management of the GÉANT network. The team plans and supervises the deployment of new systems and services, and establishes service policies and procedures. The team liaises with those NRENs connected to the network via each NREN's dedicated access port manager (APM). This channel of communication ensures the smooth management of the flow of traffic onto and off GÉANT from the connected national networks.

The operations team also oversees the working of the European distributed access (EDA) nodes for intercontinental access, and the network's interconnections with commercial IP carriers, for routing traffic to and from commercial IP addresses.

Network Operations Centre

Day-to-day management of the GÉANT network is handled by the *Network Operations Centre* (NOC) which is made up of two parts – the GÉANT *Network Control Centre* (NCC) and the GÉANT *Service Desk* (SD).

- The GÉANT SD acts as a first point of contact to receive reports of service problems and requests, 24x7, 365/366 days per year. It monitors basic network health and creates tickets for network incidents, planned maintenance and new service requests.
- The GÉANT NCC is responsible for diagnosing network problems, organising and overseeing repairs and maintenance, and configuring new services.

Building tomorrow's network

Bandwidth capacity requirements continue to grow, geographic reach needs to be extended and new networking technologies embraced so as to ensure that the network can continue to

fulfil the requirements of the research and education community and to maintain its world-leading status. In parallel with operating the existing network infrastructure, research is ongoing into those emerging technologies, standards and equipment that will be built into the GÉANT of tomorrow.

- GÉANT research teams are in collaboration with industry, standards bodies and networks around the world to identify the optimum technological solutions.
- Analysis of emerging future networking technologies and research into new services is essential to bring innovation to the core network infrastructure and technological solutions for network control, management and service-provisioning across the GÉANT Service Area.
- Examples of such new services include the provision of higher capacity bandwidth services in a static manner (e.g. at 40Gbps and 100Gbps), the provision of more dynamic circuit services (e.g. classical “bandwidth on demand”) and, looking a little further into the future, the provision of higher layer “composable” network services.

2. The European and National DCI Framework

2.1 National Grid Initiatives (NGIs) Collaboration

(C6) IGI: Italian NGI

Web Site / Document repository / Wiki: www.italiangrid.org

Contractual documents: MoU, formal support letter from the *Italian Ministry for University and Research* (MIUR) and funding deliberation available. Statute in progress

Contact person: Jru Manager, Mirco Mazzucato

6a) Description of RI

IGI is the *Italian Grid Initiative/Infrastructure*, run for the benefit of the research and education communities in Italy and worldwide. IGI, together with many European NGIs, is part of the *European Grid Infrastructure* named EGI. NGIs are "*legal organizations, supported by governments, and providing a unique representation at the European and international levels for all the communities related to national grid infrastructures: from resources providers to scientific users*". IGI is currently a *Joint Research Unit* (JRU), based on a *Memorandum of Understanding* (MoU) signed between the members in December 2007, and formally supported by the Italian *Ministry for University and Research* (MIUR) and the European Commission.

The Italian NGI IGI will soon be established as a legal national organisation (consortium) with MIUR involvement, responsible for:

- establishing, managing and operating the *national grid infrastructure* at an agreed level of service and ensuring its integration with the European e-infrastructure;
- maintaining relationships with its *national stakeholders: Research Institutes* (RIs) and Research Projects carried out by *Virtual Organizations* (VOs) constituted by *Research Teams* (RTs); *Resource Providers* (or centres) which offer resources to support the computing needs of the RTs in the country. The NGI and its Resource Providers form a national "business alliance" to jointly develop and "sell" a specific national marketplace solution (the national grid infrastructure) to their national researchers, each with its specific responsibilities;
- mobilizing the *national funding and resources* to guarantee the sustainable availability and operation of the national grid infrastructure as required by national users and to contribute to EGI.org for the common tasks;
- *representing* all its national stakeholders in the EGI Council and in relations with EGI.eu; have the capacity to sign the Statutes of EGI.org – either directly or through a legal entity representing it;
- contributing to the decisions of the EGI Council and the EGI.eu technical bodies regarding *international standards* and to the *EGI policies* and *quality criteria*, and ensuring adherence at the national level to the agreed criteria; supporting *user communities* (application independent, and open to new user communities and resource providers).

It offers more than *15,000 computing cores and storage resources* distributed across more than *50 computing centres* all over Italy. IGI brings the members of the Italian academic and research communities in contact with the latest developments in scientific computing. The Italian Grid is *one of the largest Grid infrastructures in Europe*. It is integrated with the pan-European Grid infrastructure operated in the framework of EGI and WLCG. Various resource providers are currently part of the Italian production Grid. It enables the sharing of geographically distributed resources in Italy and world-wide, such as computing, storage and data, by bridging the gap between remote resource centres and distributed communities of users. Access to resources is made possible in a standardized fashion through a customized common middleware layer based on the EGEE (now EMI) gLite stack, called INFN Grid Middleware Release.

6b) PA/NC collaboration explanation

IGI, as a national initiative, represents a collaboration between Academic and Research Institutions and the Italian *Ministry for University and Research* (MIUR).

6c) Budget, funding model, economic sustainability

Public funding from MIUR and from Partners according to the owned shares. In the future IGI aims to provide Grid services to PA and other communities (private or public bodies) and to receive financial contributions in return.

6d) Governance / Management

All partners have a representative in the *Council*, which elects a *President*, a *Director* and an *Executive Board*. The President is the legal representative of the Consortium, the Director is the executive leader and is responsible for the operation and management of the Consortium. The image below represents the organizational chart of the NGI.

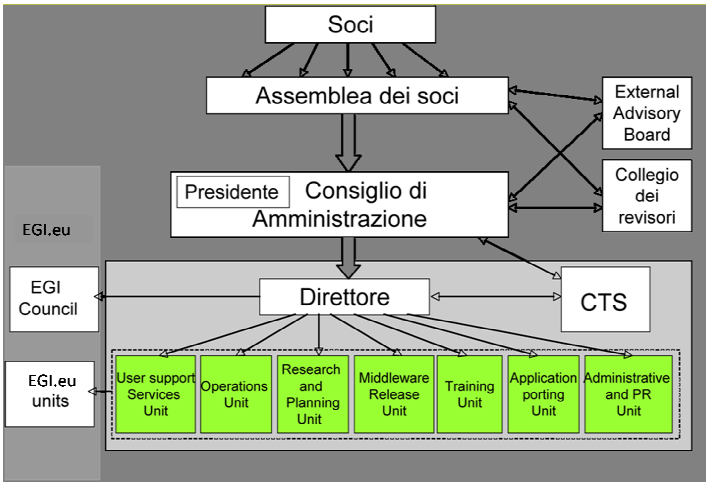


Fig. 1 – IGI Governance model.

6e) Users and interaction model

Users are organized into communities called *Virtual Organizations* (VOs). Currently, the Italian production Grid supports 49 VOs operating in different research areas such us High Energy Physics, Biology, Computational Chemistry, Bioinformatics, Earth Science, Astrophysics, etc.

The Italian production Grid is managed by a distributed operations team, which provides a help desk for Grid site managers and users and is responsible for the monitoring and planning of the infrastructure, and for the rollout of new middleware releases to sites and core Grid services.
In the future IGI will also provide Grid services to external bodies (public or private) and to Research Communities. Specific agreements will regulate these collaborations. Other scientific collaborations will be possible with institutions which have experience in development and operation of Grid Infrastructures.

6f) Countries and international collaborations

In the Italian NGI only Italian Partners are involved. IGI, as one of the European NGIs participates in the *European Grid Initiative* (EGI), whose collaboration is coordinated by EGI.eu. IGI partners (most notably INFN) are directly involved in several international (EU and extra-EU) collaborations.

6g) History and evolution

The creation of NGIs was encouraged after the end of Grid EU Projects (especially EGEE and others), in order to create a permanent European Grid e-infrastructure based on national legal organizations.

The Italian Grid Initiative was born in 2007 as a JRU, formally supported by the Italian *Ministry for University and Research* (MIUR) and the European Commission. The patronage and the funding having been assured in 2010 by the MIUR, a legal entity (Consortium) is now being created. This Consortium should be operative in 2012.

6h) Security

A range of security activities will be carried on by IGI , namely:

- definition of *Grid security policies*;
- *security challenges*: random tests at different sites in order to verify the efficiency of procedures for security crash management and the local administrator's responsibility;
- *support* to local administrators and users regarding Grid security problems;
- IGI *Certification Authority management*, which will issue X509 certificates allowing access to the infrastructures to all the authorized institutions' users;
- analysis of new models of *authentication and authorization* in the distributed computing and digital infrastructures domain, in particular in areas related to the introduction of Trust Federations and Shibboleth.

6i) Operations

Services offered by the *IGI Operations Centre* include:

- management of *central Grid services* for the efficient running of the general infrastructure and the benefit of users;
- proactive *monitoring and problem tracking* of Grid sites and services;
- operation of a middleware certification testbed to test and, validate new middleware and also to foster innovation;
- support to users and Grid site managers on middleware installation, configuration and management;
- certification of new sites;
- Grid security coordination in collaboration with EGI;
- management of a monitoring and accounting system for the national infrastructure.

The IGI Operations Centre is run by a distributed team of experts, the primary contributer of resources being the *Italian National Institute for Nuclear Physics* (INFN). It relies on the collaboration of a partner network operating under the umbrella of the Italian Joint Research Unit.

(C7) BEgrid: Belgian NGI

Web Site: www.begrid.be

Wiki: wiki.begrid.be

Contractual documents: -

Contact person: Rosette Vandenbroucke

7a) Description of RI

BEgrid is the Belgian computing/data grid for research. It offers distributed computing and storage resources for Belgian researchers by linking computing elements and storage elements via BELNET, the Belgian Research Network and using the gLite middleware to realize the grid functionality. BELNET coordinates BEgrid at the operational level and provides grid central services. It also provides the BEgrid website and wiki and organizes dissemination activities. The computing and storage resources are owned and managed by the BEgrid resource providers who are essentially universities. Slightly more than 1,100 cores are now available as worker nodes.

BEgrid is formally accepted by the federal and regional governments as the Belgian NGI. BEgrid is a member of the European Grid Infrastructure and is represented on the EGI council by the BEgrid coordinator.

7b) PA/NC collaboration explanation

BEgrid is a collaboration between BELNET, a public authority, and resource providers who can be categorized as national champions.

7c) Budget, funding model, economic sustainability

BEgrid is not a legal entity and does not have its own budget. The running costs are distributed between BELNET and the resource providers. BEgrid does not generate income, hence only expenditures are budgeted.

The minimal yearly budget can be estimated as follows:

BELNET:

Staff: 2 FTE,

Hardware: 13 K€,

EGI membership fee: 40 K€.

Resource provider:

Staff: 0,2 FTE for cluster/middleware/software maintenance,

Hardware: 50 K€ minimal.

This model is only sustainable if resource providers, such as universities and public research organizations, receive recurrent funding from the government. This financing scheme can also be coupled with a user contribution for basic and/or special services.

7d) Governance / Management

BEgrid is managed by a Management Committee consisting of a representative of each resource provider and the BEgrid Coordinator from BELNET. The Management Committee decides on the BEgrid management strategy, the provision of services and the access of users.

The Technical Committee is made up of the system managers of the grid clusters. They discuss operational aspects of BEgrid and follow up on the installation and updates of the middleware and the daily operations of their grid cluster hardware and software. They also contribute to basic user support in their organization.

BELNET coordinates BEgrid and also runs the main BEgrid services: provision of certificates, BDII, VOMS, WMS, MyProxy, UI and web portal. It also provides the Quattor service for middleware installation.

7e) Users and interaction model

Users are organized into *Virtual Communities* (VOs). BEgrid supports the international VOs CMS and e-NMR. It manages two Belgian VOs namely *betest* and *beapps*. Betest is used for courses and for users performing their first steps on the grid. Beapps is for production runs on the grid. This VO gathers all users that do not belong to High Energy Physics and Magnetic resonance for molecular research. Users in the VO beapps belong to research domains such as physical geography, photonics and medical informatics. The whole active grid user community amounts to 100 persons.

BEgrid has a distributed operations team consisting of the BELNET/BEgrid team and the grid cluster system manager at each site. The BELNET/BEgrid team also acts as the first line helpdesk for obtaining access to the grid and bringing user applications to the grid.

The High Energy Physics and e-NMR groups have their own support at all levels of grid use.

7f) Countries and international collaborations

BEgrid has a bilateral collaboration with the Dutch NGI. The Dutch NGI supports the Belgian VO beapps whilst BEgrid supports a Dutch VO. This means that members of the VO beapps are able to use computing resources in the Netherlands.

BEgrid is also collaborating with Luxemburg in the setting up of the Luxemburg NGI. Luxemburg is using the Belgian CA services and acts as a RA. BEgrid is helping to set up the User Interface and the web portal using the BEgrid *MyProxy* service. In a later phase it is planned to formulate an agreement for the reciprocal support of a VO.

BEgrid is a member of EGI as explained under a).

7g) History and evolution

BEgrid started at the beginning of 2003 by forming a "club" of organizations interested in grid computing. With private investments from mainly a few universities, a small test grid was set up. In 2005 a pilot BEgrid was set up with the Flemish Government providing funding for the necessary hardware and all involved institutes contributing human resources.

Presently BEgrid has about 1,100 cores and 100 users from four disciplines.

There are however sustainability problems as the funding has not been recurrent and there might not be enough users to secure political support for the BEgrid infrastructure.

7h) Security

BEgrid users have to accept the general grid security rules and obtain a X.409 certificate that is granted by strictly following the CP/CPS.

Access to files on the grid is managed by the Virtual Organisations service, in general files can only be accessed by members of the same VO. A finer granularity is also possible.

The security of the machines is also supervised in collaboration with the EGI Operations. Regular security updates have to be carried out on all grid clusters.

7i) Operations

Operations include both the operational work necessary at each grid cluster and also that required for the central operations of the whole BEgrid.

The operations *at each grid cluster* include:

- installation and maintenance of the grid middleware,
- follow up of security alerts,
- support to local users.

The *central operations* include:

- running the BEgrid central services: BDII, VOMS, WMS, LFC, MyProxy, User Interface, Web Portal,
- running the central middleware installation system,
- proactive monitoring of BEgrid sites,
- support to grid cluster system managers for the middleware installation,
- grid security coordination in collaboration with EGI,
- user support.

(C8) BiGGrid: Dutch NGI

Web Site / Document repository / Wiki: www.biggrid.nl

Contractual documents:

Contact person: Peter Michielse (NCF)

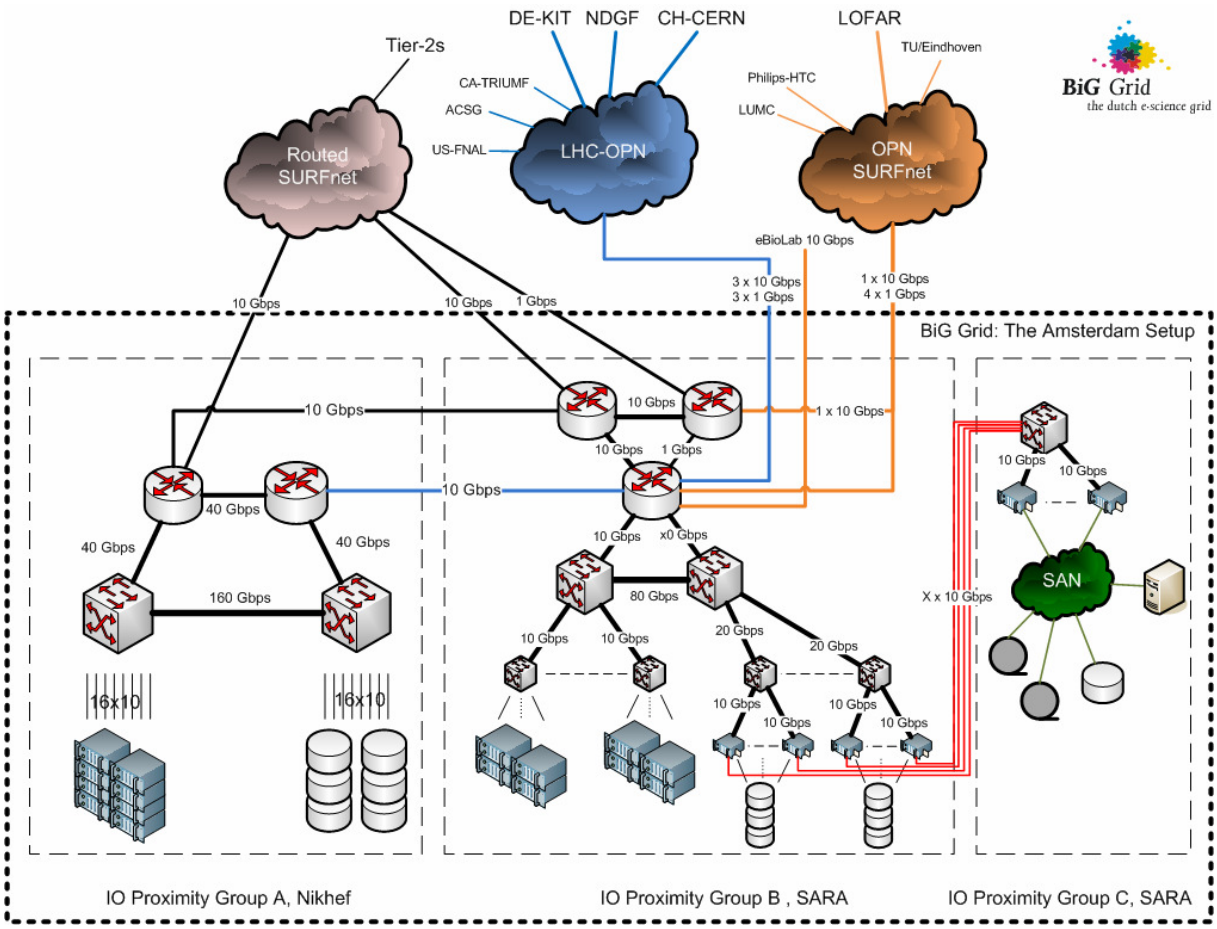
8a) Description of RI

BiG Grid is the grid infrastructure for Science and Research in The Netherlands. The "BiG Grid" project is developing this grid infrastructure to target a broad range of scientific research disciplines which are able to take advantage of the ICT resources available in a science grid infrastructure. BiG Grid, or formally the Dutch NGI which is represented by NCF, the National Computer Facilities foundation, is part of EGI, the pan-European grid infrastructure.

The founding partners of BiG Grid are NCF, Nikhef (*National Institute for Subatomic Physics*) and NBIC (*The Netherlands Bioinformatics Centre*). The other partners are SARA (*Dutch National High Performance Computing and e-Science Support Centre*), RUG-CIT (University of Groningen) and Philips Research. The founding partners signed a Collaboration Agreement in February 2009. NCF, SARA, Nikhef and RUG-CIT consequently signed a MoU defining their collaboration as a JRU.

BiG Grid has agreements with operational partners. SARA operates a large part of the BiG Grid compute, data storage and backup resources, including providing the human resources needed for both the (technical) administration of the systems and participation in BiG Grid's support and development activities. SARA also runs the Dutch National Supercomputer (HPC system) service, which has been partially funded by BiG Grid. On the High Tech Campus of Philips Research equipment has been installed accessible to the academic user community, for pre-competitive research.

The architecture of the BiG Grid resources installation at SARA/Nikhef is shown in the next figure. The number of cores at the central facility is more than 7,000 and the total storage 7,000 TB.



8b) PA/NC collaboration explanation

BiG Grid is a collaboration between several academic and research organizations and the Netherlands Organisation for Scientific Research (through NCF).

8c) Budget, funding model, economic sustainability

The BiG Grid project is funded for the period 2007-2012 by a total budget of M€ 28.8. A proposal for sustainable funding after this period, not only for the grid infrastructure but also including all other components of the Dutch high-end ICT infrastructure for scientific research, has been approved by the (previous) government but waits for a final decision by the current government on the funding model and level.

8d) Governance / Management

BiG Grid has a Board of Directors consisting of five leading Dutch researchers and a Supervisory Council in which the senior bodies of the founding partners are represented.

The BiG Grid operational organisation is referred to as the BiG Grid *Executive Team* (ET). The Board of Directors has mandated the ET to make practical operational decisions. Decisions on procurements and other significant expenditures remains at the level of the Board of Directors. The activities of the ET include:

- *Operations*. This embraces the actual purchase of hardware, including writing Request-for-Proposals and acceptance tests, actual operations of the systems, software installations, etc. The ET has delegated operational coordination to the *Operations Steering Team* (OST) which includes staff from the operational partners SARA, Nikhef, HTC Philips Research and RUG-CIT; actual operational manpower is approximately 11 FTE;
- *Support & Development*. This is not a significant concern for either the LHC-community or the Lofar-community as they are both large and well organized. Using large compute and data storage resources, however, by the usually small scale social sciences and humanities communities is however far from trivial. To steer these activities, the ET has set up a *Support & Development Steering team* (SDST) with staff from Nikhef, SARA and the (former) VL-e-project. The SDST divides the development activities over the available (software) developers, together forming the S&D team. Currently BiG Grid avails over about 12 FTE of S&D capacity. In this role, the SDST also identifies research groups for which funding of local development effort (i.e. employed by the application's home organisation) can be instrumental or even essential toward using the BiG Grid resources. Properly motivated proposals for additional S&D can be granted by the BiG Grid project, which effectively adds to the amount of FTE's in the S&D team;
- *Dissemination, website and administrative aspects*. Procedures are in place to enable researchers to apply for access to the BiG Grid resources. This is done through NWO's automated application and granting system and is taken care of by NCF. Dissemination and website activities are distributed over the ET members, with the possibility of support by external parties.

8e) Users and interaction model

Users of grid facilities usually organise themselves into *Virtual Organisations* (VOs) which are research collaborations, either national or global. Once a VO has been established and recognized, an individual user within a VO is able to use grid facilities for which the VO is eligible. Usage figures are typically collected per VO. In 2010 115 VO's were supported. The major usage of BiG Grid was by:

- *High Energy Physics*: through BiG Grid, the Netherlands operates a Tier-1 centre which stores data generated by the LHC experiment at CERN. This enables both Dutch and international scientists to analyse collision data. The research groups involved are at Nikhef, UvA, VU, UU and RU.
- *Life Sciences*: BiG Grid has rolled out distributed facilities at local research groups to start-up their e-science based scientific work. This has led to the following research subjects: location of protein activity within cells, proteomics research, bioinformatics research and DNA sequencing.

HEP uses about 70% of the resources, Life Sciences 20% and others 10%.

All Dutch researchers and research groups can apply for access to the BiG Grid infrastructure. A review of applications is currently performed by the ET. Depending on the level of experience and the user community involved, there are several possibilities means of connecting to BiG Grid:

- experienced users of grid infrastructures, who belong to existing VOs, can obtain access to the large central facilities directly, based on appropriate usage agreements. Such (also international) communities in general do not need specific application support, and have in-house expertise in using the grid and developing grid-aware application. The BiG Grid Infrastructure help desk is available for solving operational problems and maintaining the agreed service level;
- users wanting to leverage BiG Grid to enhance their applications or research, have a variety of options. For selected key applications, the BiG Grid project can make specific application support available, or assist with co-funding to attract new research disciplines to the BiG Grid infrastructure. With the help of trained *application domain analysts* the grid application bootstrap process is facilitated;
- also assistance in bootstrapping new user communities and research groups can be achieved by small hardware grid facilities, co-funded by BiG Grid, which are placed near users' own environments. When a user has embarked on the usage of grid resources through these local facilities, the next step can be taken to the usage of central facilities.

8f) Countries and international collaborations

BiG Grid facilitates scientific research in the Netherlands and has only Dutch partners. On the European level, the Dutch NGI (the JRU partners) participates in EGI, the pan-European collaboration of NGIs.

BiG Grid, both as a national project and as part of the European ecosystem, has built up valuable relationships with various ESFRI-projects. Without being complete the following can be mentioned: CLARIN, CESSDA, LIFEWATCH, BBMRI, ELIXIR, INSTRUCT, CERN, KM3NeT and PRACE.

8g) History and evolution

For years, NCF has been and still does facilitate scientific research in the Netherlands by funding high-end computing facilities, which includes supercomputing services, a national compute cluster and also grid services through the precursor projects NLGrid and NL++Grid, in which entities such as Nikhef, RUG-CIT, SARA and VL-e invested much efforts to make these successful. The BiG Grid infrastructure is an extension of these grid projects. The general aim is to facilitate the ability of many national scientific disciplines to be supported by high-end ICT infrastructure, ranging from supercomputers to grid services with specific software emanating from the VL-e project, among others.

8h) Security

The BiG Grid ET has adopted the Grid Security Policy, version 5.7a as agreed by the Joint Security Policy Group on October 10th, 2007, and constitutes the Grid Management for the purposes of the Grid Security Policy and all its subordinate Policies.

Certificates are required to authenticate services, hosts and other users in the grid environment. BiG Grid accepts certificates from all IGTF Accredited Authorities (Classic, SLCS, and MICS).

8i) Operations

The central BiG Grid resources are operated by SARA and Nikhef.

2.2 European Grid Organization and Project Collaborations

(C9) EGI.eu Organization and EGI-InSPIRE Project collaborations

Web Site: www.egi.eu

Document repository: documents.egi.eu

Wiki: wiki.egi.eu/wiki

Contractual documents: EGI Statutes (8/2/2010)

Contact person: Steven Newhouse, EGI.eu Director and EGI-InSPIRE Project Director

9a) Description of RI

Grids are a mechanism for bringing together computing and storage resources located in, and owned and operated by different organisations to ensure secure access. By connecting infrastructures via internet networks a grid is a means for sharing computer power and data storage capacity. It permits the creation of virtual research communities making use of computers located all over the globe to become an interwoven computational resource for large scale, *compute-* and *data*-intensive grand challenges.

The *European Grid Infrastructure* (EGI) is a federation of resource providers set up to deliver sustainable, integrated and secure computing services to European researchers and their international partners. EGI enables access to computing resources for European scientists and researchers from all fields of science, ranging from High Energy Physics to Humanities.

9b) PA/NC collaboration explanation

EGI.eu, a foundation recognised by Dutch law and headquartered in Science Park Amsterdam, the Netherlands, is an organisation established in February 2010 to coordinate and manage the infrastructure (EGI) on behalf of its participants: *National Grid Initiatives* (NGIs) and *European Intergovernmental Research Organisations* (EIROs).

NGIs are organisations set up by individual countries to manage the computing resources they provide to the European e-Infrastructure (EGI). NGIs are EGI's main stakeholders, together with CERN and EMBL (two EIROs). Each NGI contributes a number of sites to the grid infrastructure. NGIs are responsible for the maintenance and running of the sites they operate. NGIs are represented in the EGI.eu Council.

9c) Budget, funding model, economic sustainability

Report (preliminary) 2010:

- *income*: 1,5 M€ (1 M€ members, 0,5 M€ EC Projects);
- *expenditure*: 1,3 M€ (0,7 M€ Staff; 0,45 M€; EGI Global Tasks; 0,2 M€ Office Costs).

Budget 2011:

- *income*: 2,6 M€ (1 M€ members, 1,5 M€ EC Projects);
- *expenditure*: 2,6 M€ (0,1 M€ EGI.eu Staff; 1,4 M€ Project Efforts; 0,7 M€; EGI Global Tasks; 0,3 M€ Office Costs).

EGI.eu has three sources of *income*:

- the EC contribution towards direct (staff & travel) costs relating to funded projects;
- the EC allowance for indirect costs relating to direct costs incurred on EC projects;
- the EGI.eu participant's fees (currently set at 1 M€, with the TERENA-KEY model of contribution) towards:
  - matching the costs relating to the staff working on EC projects,
  - paying the full cost of staff working on EGI.eu business,
  - other costs of the EGI.eu organization not related to EC projects.

EGI.eu has three areas of *expenditure*:

- the staff it employs directly at EGI.eu to:
  - work on EGI.eu activities linked to the organization (as opposed to a project),
  - work on projects in which EGI.eu participates,
- the contributions it makes towards the staff employed on EGI Global Tasks located at external organizations;
- non-staff related costs at EGI.eu.

The *Executive Board* (EB) is currently proposing to increment the members' contribution in a transition scheme designed to enable the economic sustainability of EGI.eu after the end of the EGI-InSPIRE project.

The "Terena model" for NGIs & EIROs contribution was derived from the similar scheme for NRENs. It is a *band*-based scheme where NGIs (or EIROs) are categorized into classes.

9d) Governance / Management

Council & EB

EGI.eu is a foundation established under Dutch law to create and maintain a pan-European Grid Infrastructure in collaboration with the NGIs and EIROs, to guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators. EGI.eu is governed by a *Council*, which has representatives from all of its participants and is responsible for providing the long-term direction of the organisation, and the *Executive Board* which provides frequent guidance to the Director, who leads the organisation on a day-to-day basis.

For more detail, see: EGI.eu statutes, Art.6 "Council; organization and tasks", Art.7 "Council; the decision-making process", Art.8 "Executive Board", Art.9 "Tasks of the Executive board", Art.11 "Director".

Policy Groups

EGI.eu is keen to involve all relevant stakeholders in the policy development process. In practice, this means that all relevant parties, especially those affected by specific policies, will have the opportunity to be part of policy discussions, review draft proposals and provide their input during the policy making process. The policy groups operate on transparency, accountability, openness and participatory principles. Policies are developed and defined through a bottom-up approach and consensus-based decision making.

A policy group is an *internal EGI.eu body* created to define policies and procedures within a specific functional area (technology, operations, user community, policy and administration). These policy groups are responsible for developing EGI.eu's strategic and operational policy framework and, thus, for ensuring the stability and availability of a European generic e-Infrastructure.

Each policy group has well-defined responsibilities, composition and operational procedures. It is chaired by an elected or appointed member of the community who is an acknowledged expert in the relevant subject area. The chair reports the progress of the group's work to the EGI.eu management.

Active Policy Groups are:

- *Technology Coordination Board* (TCB),
- *Operational Tools Advisory Group* (OTAG),
- *Operations Management Board* (OMB),
- *Operations Automation Team* (OAT),
- *User Community Board* (UCB),
- *User Services Advisory Group* (USAG) ,
- *Security Policy Group* (SPG),
- *Software Vulnerability Group* (SVG),
- *Security Coordination Group* (SCG).

The focus will be on three relevant cases.

The *Technology Collaboration Board* (TCB) focuses on technologies that will be used within the EGI production infrastructure to deliver distributed computing services for the research communities.[3]

The *Operations Management Board* (OMB) is an advisory body which develops strategy and technical priorities concerning the deployment and operation of production infrastructure, oversees the status and progress of the global EGI operational services and of the NGI operational services.[4]

The purpose of the *User Community Board* (UCB) is to be the focal point within EGI for identifying and resolving issues relating to User Communities.[5] UCB provides a forum for end-users in structured user communities to shape the infrastructure for their needs. This includes defining the policies relating to their use of the infrastructure and by identifying and prioritizing the requirements and issues relating to their use of EGI's production infrastructure. User communities in EGI are recognized through *Virtual Research Communities* (VRCs) as this provide a means for grouping aligned *Virtual Organizations* (VOs) that use the infrastructure in order to provide:

- technical feedback on the services offered by EGI to its users,
- requirements to EGI for new and enhanced services.

EGI-InSPIRE Governance

The Governance structure of EGI-InSPIRE comprises the following bodies:

- the coordinating body EGI.eu, represented through the *Project Director* (PD) and the *Project Office* head-quartered in Amsterdam,
- the *Collaboration Board* (CB) representing the partners in the project,
- the *Project Management Board* (PMB) representing groups of partners; being smaller than the CB, the PMB is able to focus on tactical managerial issues,
- the *Project Administration Committee* (PAC) set up to monitor the reporting process,
- the *Activity Management Board* (AMB) composed of the activity leaders, who oversee the day-to-day progress of the project's work, and
- the *External Advisory Committee* (EAC) composed of internationally recognised experts who are both users and providers of e-infrastructures, which advises the PMB and the PD on the relevance of the Project plans in a world-wide context.

[3] See "TCB terms of reference" in documents.egi.eu.
[4] See "OMB terms of reference" in documents.egi.eu.
[5] See "UCB terms of reference" in documents.egi.eu.

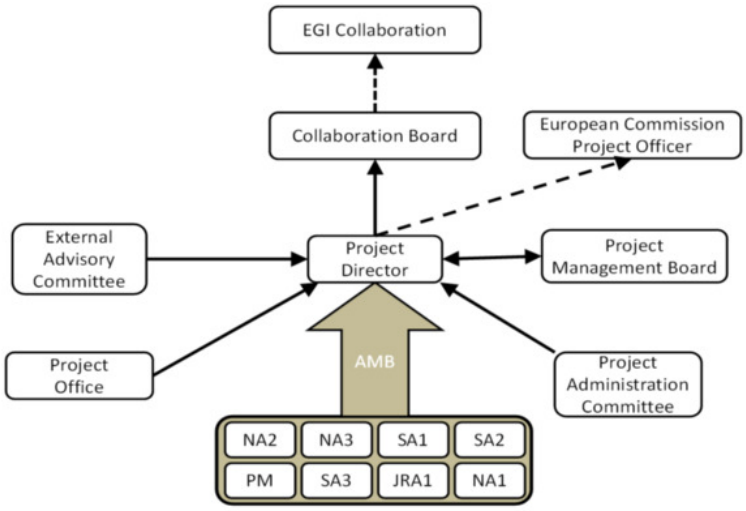


Fig. 2 – Project EGI InSPIRE governance.

9e) Users and interaction model

The federated resources provided by EGI are available to all scientists and researchers who are members of a *Virtual Organisation* (VO). Each VO has its own rules as to who can join their community and membership may be open to non-European collaborators.

The resources coordinated by EGI are free at point of use: individual users do not have to pay to use the grid infrastructure. Participating countries and institutions contribute to the common costs of running the infrastructure. The individual resource providers (NGIs) fund and maintain the hardware in their own countries

In EGI there are currently 13,699 users (+35% from April 2010), grouped into 218 VOs (+25% from April 2010). As of April 2010, 15 million jobs/month were running in 52 countries over 317 sites, using nearly 250,000 cpu cores. The scientific disciplines involved are: astronomy and astrophysics, computational chemistry, computer science and mathematics, earth sciences, fusion, HEP, Infrastructure, Life Sciences and others.

Application domain	Number of active VOs	Number of users
Computer Science and Mathematics	8	10
Multidisciplinary VOs	34	1988
Astronomy, Astrophysics and Astro-Particle Physics	22	344
Life Sciences	17	748
Computational Chemistry	5	481
Earth Sciences	13	320
Fusion	2	16
High-Energy Physics	45	5922
Infrastructure	31	1759
Others	41	2111
TOTAL	**218**	**13699**

Fig. 3 – EGI VOs/Users data (updated on Feb 9th 2011, source: cic.egi.eu).

The users are mainly from Academia / Research Institutions.

User Access:[6]

The first step towards becoming a user is to join a *Virtual Organisation* (VO). For that, one needs to: (1) obtain a personal grid certificate that authenticates the user within the grid infrastructure and grants access to computing, storage and other types of resources. This can be done through the local grid Certificate Authority in the home country, which can be found through the webpage of the International Grid Trust Federation. Then, (2) choose a VO to join and access the resources of the grid infrastructure. VOs group users by scientific discipline, grid use case or geographical region. The list of registered VOs can be obtained from the Operations portal.

The registration is reviewed by the User Community Board of EGI, which then approves the request if the proposed VO does not overlap with the scope of existing VOs. EGI will support the connection of computing, storage and other types of resources provided by the scientific domain that the approved VOs wishes to use.

Community Access:[7]

International scientific communities can benefit from a strong partnership with EGI if they are organised as *Virtual Research Communities* (VRC). A VRC represents a community of researchers with an established presence in its scientific or other research field, for example an ESFRI project, EIROFORUM laboratory or national research structure. VRCs have an established governance model and open mechanisms for new participants to enter (or leave) the VRC. They also guarantee that all their members have access to the services offered by the VRC.

When these conditions are met, the VRC is recognised as the 'voice' of a given community of users within EGI. EGI is then able to better serve the needs of that community by introducing new services and support processes in response to the defined and prioritised needs of the VRCs.

9f) Countries and international collaborations

The *EGI Council* is composed of the following members:

BELNET Belgium BE , IPP-BAS Bulgaria BU, SWITCH Switzerland CH, CESNET Czech Republic CZ, CyGrid Cyprus CY, Gauß-Allianz Germany DE, DCSC Denmark DK, EENet Estonia, CSIC Spain ES, CSC Finland FI, CNRS France FR, GRNET Greece GR, SRCE Croatia HR, NIIF Hungary HU, Grid-Ireland Ireland IE, IUCC Israel IL, INFN Italy IT, RESTENA Luxembourg LU, LUMII Latvia LV, UoM Montenegro ME, MARGI Macedonia MK, NCF the Netherlands NL, UNINETT Sigma AS, CYFRONET AGH, UMIC Portugal PT, ICI Romania RO, IPB Serbia RS, ARNES Slovenia SI, SlovakGrid Slovakia SK, SNIC Sweden SE, ULAKBIM Turkey TR, JISC United Kingdom UK, CERN EIRO.

The European Project collaboration EGI-InSPIRE is a consortium of 50 partners, including 37 National Grid Initiatives (NGIs), two European International Research Organisations (EIROs) and eight partners from the Asia Pacific region.

[6] Procedure from: www.egi.eu/user-support/becoming_a_user.
[7] Procedure from: www.egi.eu/user-support/becoming_a_community.

International collaborations

The currently active international grid collaborations are indicated in the following figure:

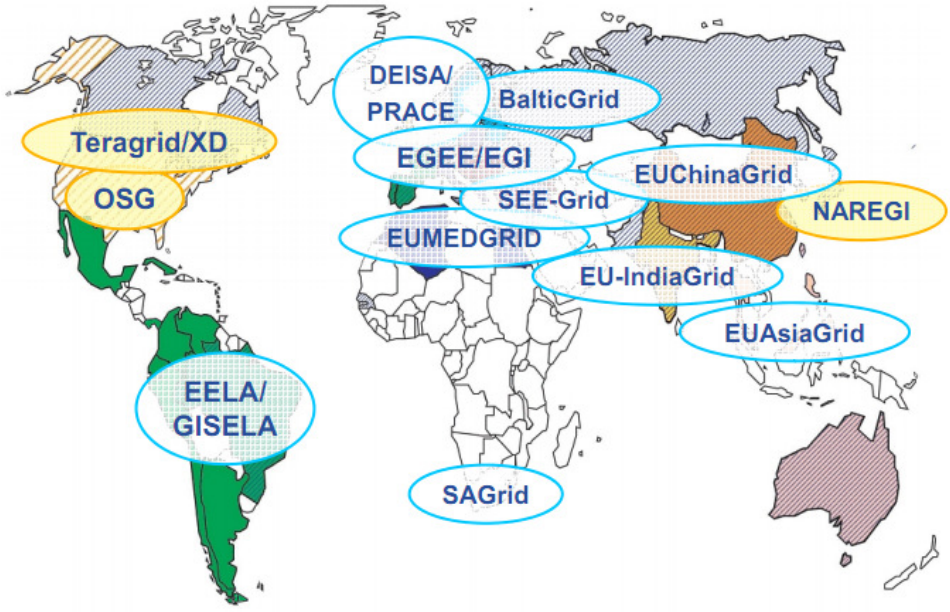


Fig. 4 – Grid international collaborations.

Other collaborations

Each external collaboration is formalised via a *Memorandum of Understanding* (MoU), i.e., a signed document written to confirm and define the framework of collaboration between EGI.eu and individual partners.

The EGI.eu recognises MoUs as tools to open wide and long-term activity and cooperation with partners. Such collaborations ultimately bring visible benefits to scientists and researchers. In addition, external collaborations will be formalised through membership and participation in international policy bodies.

The EGI.eu is working to establish collaborations with external partners in the following categories:

- Technology providers, with the *European Middleware Initiative* (EMI) and the *Initiative for Globus in Europe* (IGE),
- European and International e-Infrastructure providers,
- Dissemination/coordination projects, with e-Science Talk,
- International policy bodies, with *Open Grid Forum* (OGF), *e-Infrastructure Reflection Group* (e-IRG), *European Policy Management Authority for Grid Authentication in e-Science* (EUGridPMA),
- *Virtual Research Communities* (VRCs).

9g) History and evolution

EGI.eu was created in February 2010 to coordinate and maintain a sustainable pan-European infrastructure to support European research communities and their international collaborators. Its work builds on previous EU-funded projects which nurtured this goal, commencing from the initial concept of a scalable, federated, distributed computing system.

The distributed computing grid was originally conceived in 1999 to analyse the experimental data produced by the Large Hadron Collider at CERN – the European particle physics laboratory located on the Swiss/French border.

The European *DataGrid Project*, which started in January 2001, led the research and development of Grid technologies. It established the organisational structure, gathered and analysed requirements, developed middleware (the software that links hardware resources), and provided training to its users. The project proved the Grid's successful application in various research fields – high energy physics, earth observation and bioinformatics. Upon completion in March 2004, a new project called EGEE (*Enabling Grid for E-sciencE*) took over the Grid's further development in what would result in three successive two-year phases.

EGEE provided researchers with access to computing resources on demand, from anywhere in the world and at any time of the day. Ease of access and the ability to analyse a larger amount of data within a shorter timescale than before attracted participation from a wider range of scientific disciplines. By April 2010 when the last EGEE project phase was completed, there were about *13 million jobs per month* running on the Grid, hosted by a network of *300 computer centres* worldwide.

A dedicated design study (EGI-DS, *European Grid Initiative Design Study*) took place from September 2007 to December 2009. It established the conceptual and logistical framework for a permanent organisation to oversee the operation and development of the Grid on a Europe-wide level.

9h) Security

There are several procedures regarding security in EGI. As EGI is a *distributed* infrastructure, security is a strong requirement in order to have a reliable and trustworthy management of grid applications (running as jobs) and data. Security is *built-in* to the middleware, using several, sometimes stack-dependent[8], technologies, such as X.509 PKI public/private key pairs for credentials and CAs, Shibboleth, Kerberos, OpenID, *proxies* or SAML ETD for trust delegation, VOMS or UVOS for Virtual Organization management, Argus for authorization. Guidelines are expressed in the EGI Grid Security Policy document[9].

Grid Management

The management provides, through the adoption of this policy and through its representations on the various approving bodies of the Grid, the overall authority for the decisions and actions resulting from this policy including procedures for the resolution of disputes.

[8] Middleware *stacks* are, for instance, gLite, ARC, UNICORE, dCache, globus, …
[9] See: https://documents.egi.eu/document/86.

Grid Security Officer and *Grid Security Operations* The management appoints a Grid Security Officer who leads and/or coordinates the team providing the operational security capability, known as Grid Security Operations.

The Grid Security Officer may, in consultation with Grid Security Operations, management and other appropriate persons, require actions by participants as are deemed necessary to protect resources from or contain the spread of grid security incidents. The responsibilities of Grid Security Operations include:

- the maintenance of contact details of security personnel at each participating site and the facilitation of Grid-related communications between them,
- handling of operational security problems as they arise,
- providing incident response teams who will act according to the Security Incident Response Policy,
- handling requests for exceptions to this policy.

Virtual Organisation Management

The responsibilities of the VO management include:

VO Security Policies: VOs are required to abide by the Virtual Organisation Operations Policy and the Virtual Organisation Registration Security Policy. They must have a VO *Acceptable Use Policy* (AUP) and ensure that only individuals who have agreed to abide by the Grid AUP and the VO AUP are registered as members of the VO.

User Registration and VO Membership Service: The user registration procedure of the VO is required to be consistent with the Virtual Organisation Membership Management Policy. Approval to join the VO must be restricted to individuals who are recognised as having legitimate rights to membership and who agree to be bound by the AUPs. A VO membership service must be provided with appropriate interfaces to generate authentication, authorization and other identity mapping data for the services running on the sites. VOs are required to maintain the accuracy of the information held and published about their members, and to promptly remove individuals who lose their right to such membership.

VO-specific Resources: VOs are responsible for ensuring that their software does not pose security threats, that access to their databases is secure and sufficiently monitored, that their stored data are compliant with legal requirements and that VO-specific services are properly monitored and do not compromise sites or resources.

Applying Sanctions to Users: VOs are responsible for promptly investigating reports of users failing to comply with the AUPs and for taking appropriate action to ensure future compliance.

Site Management

The responsibilities of the Site management include:

Site Operations Policy: Sites hosting resources are required to provide reliable and well managed services and abide by the Grid Site Operations Policy. Sites must abide by the Site Registration Security Policy and the Grid Security Traceability and Logging Policy.

Mitigating Risks: Sites acknowledge that participating in the Grid increases the risk arising from security incidents, to both Grid and non-Grid hosts on each site. Sites are responsible for mitigating this risk.

Incident Response: Sites accept the duty to cooperate with Grid Security Operations and others in investigating and resolving security incidents, and to take responsible action as necessary to safeguard resources during an incident in accordance with the Security Incident Response Policy.

Access Control: Access to all resources is controlled by a common grid security infrastructure which includes both authentication and authorization components. The global components of this infrastructure, e.g. as specified in the Approval of Certification Authorities, must be deployed by all sites and resources. The deployment of additional local security measures is permitted should the local security policies of the site or resource administration require this.

Notification of Legal Compliance Issues: If exceptions or extensions to this policy are required because of local legislation, the site must inform the Grid Security Officer.

Resource Administrators: In addition to their local site policy, resource administrators must ensure their implementations of services comply with this policy.

The responsibilities of resource administrators include:

Notifying Site Personnel: Resource administrators are responsible for ensuring that their site is registered with the Grid and that all appropriate personnel concerned with security or system management at their site are notified of and accept the requirements of this policy before offering any services.

Resource Administration: The resource administrators are responsible for the installation and maintenance of resources assigned to them, including ongoing security, and subsequently for the quality of the operational service provided by those resources.

Physical security

All the requirements for the physical security of resources are expected to be adequately covered by each site's local security policies and practices. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards.

Stronger physical security may be required for equipment used to provide certain critical services such as VO membership services or credential repositories. The technical details of such additional requirements are contained in the procedures for operating and approving such services.

Network security

All the requirements for the networking security of resources are expected to be adequately covered by each site's local security policies and practices. These should, as a minimum, reduce the risks from intruders and failures of hardware or software by implementing appropriate firewall protection, by the timely application of all critical security-related software patches and updates, and by maintaining and observing clearly defined incident response procedures. It is Grid policy to minimise the security risk exposed by applications which need to communicate across the Internet; even so, the peripheral firewall on every

participating site may be required to permit the transit of inbound and outbound packets to/from certain port numbers between a number of external and internal hosts in order to run or reach services.

9i) Operations

The EGI Infrastructure is the composition of a *Resource Infrastructure* and a *Service Infrastructure*. The Resource Infrastructure is constituted as a federation of multiple Resource Infrastructures, which in turn are a federation of local *Resource Centres*. Resource Infrastructure *Operations Managers* are members of the OMB. The OMB is the body responsible of leading the evolution of EGI operations through the periodic gathering, discussion and prioritisation of requirements, which are further reviewed by the TCB together with the user requirements.

The EGI Service Infrastructure comprises *Global and Local Services*, which are under the technical responsibility of EGI.eu and the *Operations Centres* respectively. The exchange of operational services at different levels is regulated through the definition of OLAs, which technically define the services, the associated quality level to be delivered, and other obligations of the partners. The EGI operations stakeholders contribute to innovation through their requirements that are periodically gathered, discussed, and prioritised in the framework of the OMB and of the TCB. New requirements are necessary to evolve established procedures and policies, to ensure that the deployed software meets the needs of users and Resource Centre administrators, and to ensure the advancement of Local and Global services.[10]

EGI rests on two pillars: the *Resource Infrastructure* and the *Service Infrastructure*.

Resources are geographically distributed, and are contributed by *Resource Centres*. A Resource Centre is the smallest resource administration domain within EGI. A *Resource Infrastructure* federates one or more Resource Centres to constitute a homogeneous operation domain. The Resource Infrastructure usually encompasses heterogeneous resource types, currently these are mainly *high throughput computing*, *high performance computing*, and *storage*, which are seamlessly made accessible through the deployment of standard interfaces and gateways provided by various Grid middleware stacks such as ARC, gLite, UNICORE and Globus. Other resource types will be integrated as technologies mature during the project, such as instruments, digital repositories, Desktop Grids and virtualization.

The *Service Infrastructure* enables a secure, interoperable and reliable access to distributed resources. EGI services are provided locally by *Operations Centres* and globally by EGI.eu. *Local and Global Services* are mutually dependent, and can be complemented by additional services customised for local VOs and local *Resource Centres*.

[10] See: EGI Document 218-v9 D4.1 Operations Architecture, https://documents.egi.eu/public/ShowDocument?docid=218.

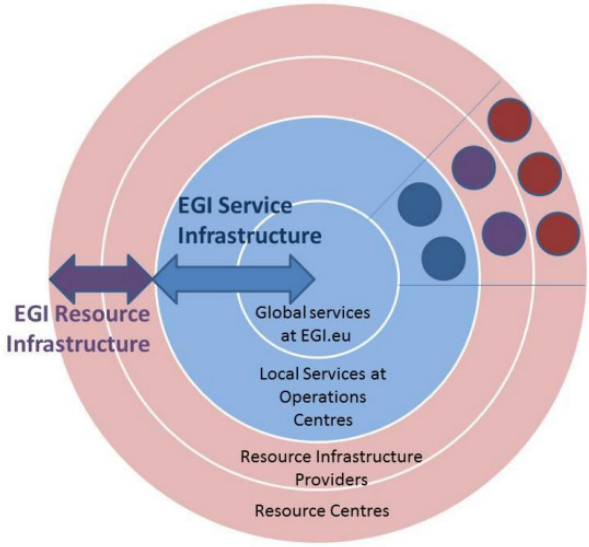


Fig. 5 – The EGI Operations Architecture

EGI's facilities for *usage accounting, monitoring and support*, are distributed in nature and constituted as a central set of services which are complemented by local services operated by the various Operations Centres. This tiered architecture is generally applicable to all of EGI's operations services, including the development, maintenance and enforcement of a common set of procedures, policies and best practices, Grid oversight, coordination of software deployment, interoperation, first-line support, the provisioning of core middleware services, and operations security.

2.3 Middleware Providers' Collaborations

(C10) The EMI Grid Middleware Provider collaboration

European Middleware Initiative

Web Site: www.eu-emi.eu

Document repository & wiki: twiki.cern.ch/twiki/bin/view/EMI

Contractual documents: EMI Grant Agreement n. 261611, 2010-07-05 – Annex DoW

Project Director: Alberto Di Meglio

10a) Description of RI

The *European Grid Infrastructure* (EGI) is a federation of resource providers set up to deliver sustainable, integrated and secure computing services to European researchers and their international partners. EGI enables access to computing resources for European scientists and researchers from all fields of science, ranging from High Energy Physics to Humanities.

The *European Middleware Initiative* (EMI) is a collaboration of the three major middleware providers in Europe, ARC, gLite and UNICORE, and other consortia. EMI aims to *deliver a consolidated set of middleware components for deployment* in EGI, PRACE and other DCIs; extend the interoperability between grids and other computing infrastructures; strengthen the reliability of the services; and establish a sustainable model to maintain and evolve the middleware, fulfilling the requirements of the user communities.

European scientific research has benefited recently from the increasing availability of computing and data infrastructures with unprecedented capabilities for large scale distributed initiatives. These infrastructures are largely defined by enabling middleware. After the necessary initial period of research and consolidation that has taken place over the past several years, the growing usage of these resources now requires the transformation of the computing infrastructures into a professionally managed and standardized service. It is of strategic importance for the establishment of permanent, sustainable research infrastructures to lower the technological barriers still preventing resource owners from federating the resources, and potential communities of tens of thousands of researchers from using grids as a commodity tool in their daily activities.

The EMI *project* will make the realization of this vision possible by addressing a number of problems that *still prevent users from easily accessing and using the whole capacity of the existing computing infrastructures*. It will focus on *improving the usability and accessibility for scientific users and the interoperability and manageability for service providers*.

The *sustainability of the grid services* will be directly addressed by *replacing, wherever possible, proprietary technology with off-the-shelf components*, improving their standardization and implementing industry standard quality assurance methodologies.

10b) PA/NC collaboration explanation

EMI and EGI-InSPIRE are two of the six projects funded under “Distributed Computing Infrastructures” sub-topic of the e-Infrastructures topic of the FP7 “Capacities” Specific Programme Call 7 (FP7-Infrastructures-2010-2), which closed in November 2009. The other four are:

- **IGE**, the *Initiative for Globus in Europe* which provides the European link with Globus technology. A close collaboration with IGE will ensure better interoperability and convergence on standards. It will also ensure that those components within the EMI stack with Globus dependencies can be more effectively supported.
- **EDGI**, the *European Desktop Grid Initiative* will develop bridge middleware that integrates ARC-, gLite- and UNICORE-based Grids with Desktop Grids (BOINC and XtremWebHEP-E). Interoperability of grid services with desktop grid technology already began with gLite during the EGEE III project. The EMI

collaboration with EDGI will further extend this to ARC and UNICORE, and in general all the middleware services supported by EMI where possible.

- **StratusLab** will incorporate *virtualisation and cloud technologies* into existing and future grid infrastructures. The StratusLab Toolkit will benefit infrastructure operators through simplified administration, increased flexibility, and improved resilience. For research communities, StratusLab will improve the usability of distributed computing resources, attracting scientific and industrial users who have embraced the cloud computing model. It will also strengthen European know-how in virtualisation and cloud technologies. EMI aims to have a strong relationship with this project in order to ensure that the EMI components can actually be used within virtualized environments being also compatible with cloud technologies.
- **Venus-C** will develop and deploy *a Cloud Computing service for research and industry communities in Europe*. This will offer an industrial-quality service oriented platform based on virtualisation technologies. The project aims to enable easy deployment of end-user services, thus making e-Infrastructures more widely useful to a range of research fields. The project will be industry led and will have access to *Microsoft Azure*, a major commercial Cloud service. In this context, it is expected that there will be a fruitful exchange of know-how between EMI and Venus-C in the field of Cloud computing and technologies.

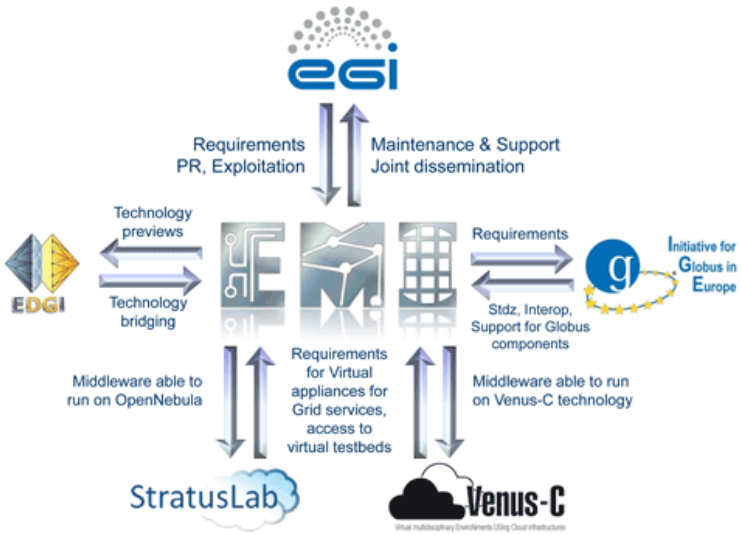


Fig. 6 – Collaborations of EMI with EGI and the other middleware providers.

The six "DCI Projects" have come together on several occasions, in particular during the "Engaging European DCIs Together" workshop organised by the SIENA project in May-June 2010. As a result of an ongoing joint discussion, the parties have produced a written *DCI Collaborative Roadmap* that aims to harmonize these core technologies and thus strengthen and broaden the set of services underpinning all distributed computing activities. In particular, the integration of core middleware services such as those provided by EMI and Globus with Desktop Grids and Cloud-related toolkits will establish a new level of pervasiveness for distributed computing.

10c) Budget, funding model, economic sustainability

Project funded by the CE, Combination of CP & CSA.

Duration: 36 months. Total costs: 24 M€.

10d) Governance / Management

The EMI *Project Execution Board* (PEB) is responsible to assist the *Project Director* (PD) in the execution of the project plans and in monitoring milestones, achievements, risks and conflicts within the project. It is led by the PD and is composed of the *Deputy Project Director*, the *Work Package Leaders*, the *Technical Director* and the *Deputy Technical Director*.

The *Executive Collaboration Board* (ECB) is a consulting committee within the CB composed of two representatives from the CB for each of the participating middleware consortia (ARC, gLite and UNICORE). The ECB represents the CB in all the situations where a full participation of all beneficiaries is not required and a faster decisional process is necessary to assist the PD in short-term or for urgent matters, mainly on non-contractual issues concerning the relationships among the Middleware Consortia. The ECB is also the first escalation step in the resolution of grave technical disagreements between the Project Director and other members of the project. The ECB chair is rotated, with each middleware consortium taking a turn.

The *EMI Project Technical Board* (PTB) is led by the *Technical Director* (TD) and composed of the *Technical Area Leaders* and a representative. It is responsible to assist the TD in defining the technical vision of the project and deciding on specific technical issues. The PTB members are the coordinators of the project Technological Areas. The PTB can invite experts (e.g. product team leaders, component developers, etc.) or delegate specific tasks to appointed working groups as required.
The *Engineering Management Team* (EMT) is lead by the Release Manager and composed of the Product Team Leaders (or duly appointed representatives), a *Quality Assurance* (QA) representative, a Security representative, representatives of the Operations teams of the major infrastructures (EGI, PRACE, etc.) and invited experts as necessary. The role of the EMT is to manage the release process and the 'standard' changes, that is all the changes that are pre-approved based on established policies and do not need to be individually approved by the PEB or the PTB. This includes software defects triaging and prioritization, technical management of releases, integration issues, and user support request analysis. The EMT is therefore the natural aggregation point for all PTs to discuss practical integration and release issues and is adapted to the largely distributed nature of the project. This mechanism has already been successfully employed in other very distributed projects, like EGEE III. The Release Manager reports to the SA1 Work package leader.

Project Director (PD): responsible for the overall project administrative and executive management and for interfacing with the European Commission. The Project Director is appointed by the coordinating beneficiary (CERN). The PD is responsible to execute the overall project plans, monitor the progress of the Work Package Leaders on project activities with respect to expected technical achievements, results, schedule, resource consumption and risks and eventual contingencies. The PD reports to the project Collaboration Board and produces quarterly and annual consolidated reports to the European Commission.

Technical Director (TD): decides on specific technical matters within the project and leads the Project Technical Board. The TD is nominated by the CB and reports to the PD as part of the PEB. In case of strong persistent disagreement between TD and PD, the issue is handled by the Executive Collaboration Board and ultimately handled by the Collaboration Board for a final decision. The TD has the role of Deputy of the Project Director and the JRA1 Work Package Leader is Deputy TD.

Work Package Leader (WPL): responsible for coordinating the operations of each Work Package and in particular to ensure that the project schedule is maintained, notifying the PD of any discrepancy; ensure that the objectives and results of the activities within his/hers Work Package are achieved, and that the deliverables for the EC are available according to the programme; arrange technical reviews of specific milestones as required by the PD or the EC; ensure technical liaison for the work in his/her Work Package with the PD and the rest of the project through dedicated meetings and events; provide the PD with all the information related to the Work Package, outlining progress within such Work Package and highlighting all problems and actual or expected delays. The WP Leaders delegate most of the execution of the software development and support to the EMI Product Teams, which keep the WP Leaders informed of the status of the assigned technical objectives.

Task Leader (TL): responsible for managing specific tasks within a Work Package and assist the WPL in the management of the Work Package. The TL is proposed by the PD and approved by the CB.

Technical Area Coordinator (TAC): the members of the Project Technical Board responsible for the overall coordination of each of the four technical areas. The TAC are responsible to define together with the relevant Product Team Leaders the technical strategy of their area. They are also responsible to define together with the TD and the other TACs the overall project technical plans. The TAC are proposed by the PD and the TD and approved by the CB.

Product Team Leader (PTL): responsible for managing a specific Product Team. The PTL is delegated responsibility for execution of one or more technical tasks the by the Work Package leaders. Each Product Team can span the activities of one or more Work Package and therefore receive delegation for different tasks by different Work Package leaders. Typically, a Product Team Leader is responsible for the design and development of specific products as part of JRA1 and for the support and maintenance of specific products as part of SA1. The PTL therefore reports to the SA1 leader and the JRA1 leader for the execution and achievement of the assigned tasks within each WP. This is reflected by the fact that technical personnel in each PT can spend effort in SA1 or in JRA1 depending on the specific task to be executed. The PTL or a duly appointed representative participates to the works of the EMT and the PTB. The effort spent by each project member is reported to the EMI Project Office using the monthly timesheets and is accounted against the Work Breakdown Structure described in the project DoW In this respect, the PTLs are not requested to report the effort spent by the PT to the WP leaders. However, the estimated allocation of effort between maintenance and support tasks (SA1) and development tasks (JRA1) will be monitored by the PD and the WP leaders and the PTLs can be requested to explain any substantial deviation from the initial estimates.

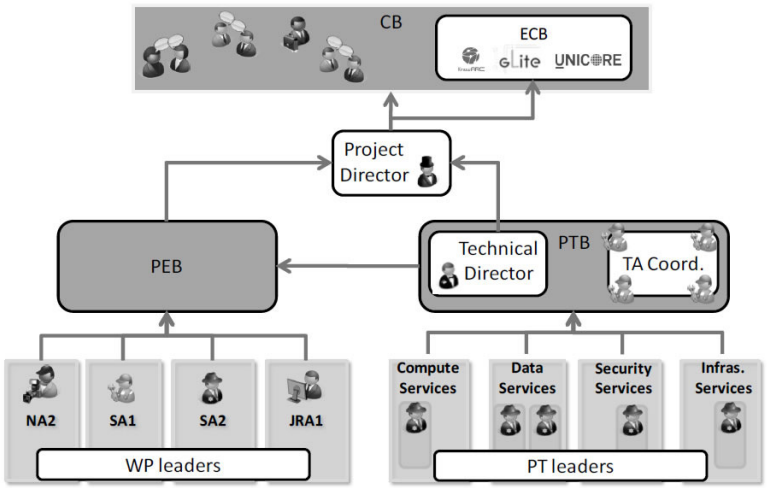


Figure 1: The EMI Project Management Structure

Fig. 7 – EMI Project Management Structure - (*see:* twiki.cern.ch/twiki/bin/view/EMI).

10e) Users and interaction model

We recall here that in EGI there are currently 13,699 users (+35% from April 2010), grouped in 218 VOs (+25% from April 2010). As of April 2010 15 million jobs/month were running in 52 countries over 317 sites, using nearly 250,000 cpu cores. *EMI users* should be considered both *sites and job submitters*. There is currently no data regarding the specific usage of each middleware – in this transition phase, there are different accounting systems for gLite, UNICORE and ARC. By using the BDII Information System, it should be possible in the near future to obtain detailed usage figures regarding the different middleware flavours used.

10f) Countries and international collaborations

EMI's main customers are the major European and international infrastructure projects, scientific user communities developing applications to run on the infrastructures and making use of the middleware services, standardization bodies and commercial companies offering distributed computing services to their customers.

The primary target is represented by major European and international infrastructure providers, including but not limited to:

- EGI, currently *the major customer and source of requirement* for EMI. The two have closely collaborated since the initial phases of the proposal preparation activities and are now formalizing their relationship with concrete common initiatives. The activities of collecting and analysing requirements and delivering software products and support services are organized through a number of formal mechanisms, including Requirements analysis and technical roadmaps, Software releases and User support.
- PRACE, another important source of requirements for EMI, particularly in the domain of *High Performance Computing* (HPC). Members of the project preparation teams of EMI and PRACE have collaborated since the initial phases of the proposal preparation activities and are now formalizing their relationship.

- WLCG which is the *largest and most active user community* using the EMI middleware services. Although a large part of the infrastructure and services used by WLCG are managed by sites participating in EGI, WLCG has expressed the need to directly control the process of defining new requirements and implementing them in future middleware services. To this end, WLCG is establishing a technical board that will collect and analyse the requirements of the HEP community and make recommendations on how the middleware services (and also other software) have to evolve.
- OSG (*Open Science Grid*, an US grid network), which has *a long history of collaboration with European infrastructure projects* especially with EGEE. During the preparation phase of the EMI project, contacts were established with OSG representatives to collect feedback and make sure that the collaboration would continue after the transition from EGEE to EGI and EMI. OSG and EMI are engaged in technical and strategic collaborations.

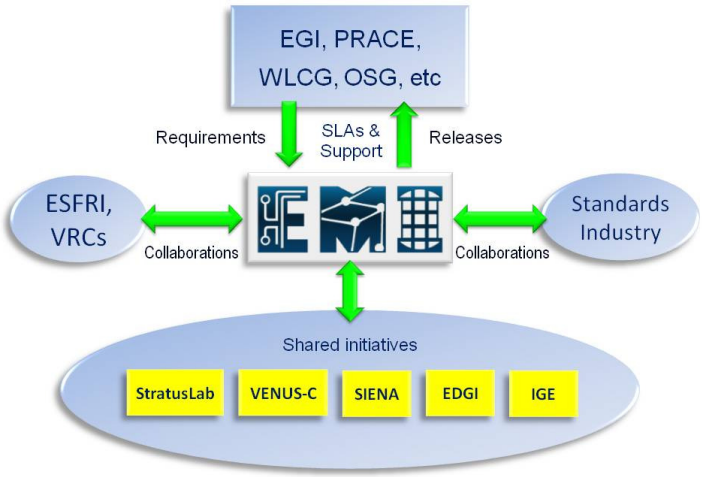


Fig. 8 – External collaborations involving currently EMI.

The project members of EMI are:

- *European Organization for Nuclear Research* (CERN) Switzerland,
- *Centro de Supercomputación de Galicia* (CESGA) Spain,
- CESNET, *zajmove sdruzeni pravnickych osob* Czech Republic,
- CINECA - *Consorzio Interuniversitario* Italy,
- *Agencia Estatal Consejo Superior de Investigaciones Cientificas* (CSIC) Spain,
- *Deutsches Elektronen-Synchrotron* (DESY) Germany,
- *Fundamenteel Onderzoek der Materie* (FOM) The Netherlands,
- *Forschungszentrum Jülich GmbH* (FZJ) Germany,
- *Greek Research and Technology Network SA* (GRNET) Greece,
- *Istituto Nazionale di Fisica Nucleare* (INFN) Italy,
- *Lunds Universitet* (LU) Sweden,
- *National Information Infrastructure Development Institute* (NIIF) Hungary,
- *Science and Technology Facilities Council* (STFC) United Kingdom,

- *Teleinformatikdienste fuer Lehre und Forschung* (SWITCH) Switzerland,
- *Trinity College Dublin* (TCD) Ireland,
- *Technische Universität Dresden* (TUD) Germany,
- *University of Copenhagen* (UCPH) Denmark,
- *University of Helsinki – Helsinki institute of Physics* (UH.HIP) Finland,
- *Universitetet i Oslo* (UiO) Norway,
- *Univerzita Pavla Jozefa Šafarika V Kosiciach* (UPJS) Slovak Republic,
- *Uppsala Universitet* (UU) Sweden,
- *Uniwersytet Warszawski* (UWAR) Poland,
- *Korea Institute of Science and Technology Information* (KISTI) South Korea,
- *Academia Sinica Grid Computing* (ASGC) Taiwan.

10g) History and evolution

After the necessary initial period of research and consolidation that took place during the past several years especially with EGEE and OMII-EU Projects, the growing usage of these resources now requires the transformation of the computing infrastructures into a professionally managed and standardized service. It is of strategic importance for the establishment of permanent, sustainable research infrastructures to lower the technological barriers still preventing resource owners from federating the resources, and potential communities of tens of thousands of researchers from using grids as a commodity tool in their daily activities.

10h) Security

For EMI, a particularly sensitive issue (from the middleware point of view) is *security management*. Although the use of *certificates* or *proxies* is established as an efficient mechanism to manage security credentials and roles, *the overhead for end-users in getting and managing certificates is still one of the major barriers for many users*. Different security methods based on systems like Shibboleth or Kerberos are used in many academic and research infrastructures for non-Grid resource access. Commercial use of the grid middleware *is even more affected* by the current complexity of the security mechanisms.

EMI aims at developing middleware that strengthens the European presence by consolidating existing DCIs and improving the stability, usability, security and quality of service. To this extent, EMI has identified the following tasks:

- identify common layers of functionality in its middleware services and actively work on producing *common components and libraries* across the three middleware stacks;
- simplify the management of security credentials by *reducing the complexities of handling certificates* and *integrating different security mechanisms* like Shibboleth and Kerberos across the three middleware stacks;
- define, improve, implement and validate *common standards* for the most important middleware functions, like *job management*, *data management* and *information management* in collaboration with relevant standardization initiatives, but with primary focus on their functional and operational aspects;

- establish a common, measurable *software certification process* based on best practices and put it at the base of the *Service Level Agreements* (SLA) with infrastructure providers and users;
- provide a *common repository* of *certified middleware components*, *test suites* and *documentation* to allow users and application and services providers, also from commercial initiatives, to take informed decisions about their requirements and usage criteria.

The innovations in Grid security will focus on *improvements in usability and transparency for users* and a transition to a *common security solution based on industry standards*. EMI will develop a *common security infrastructure* for the middleware components and services. In order to achieve this, the communications and security tokens passed between different services will be rationalized. Communication between services will be enabled by the use of industry standard SSL/TLS instead of the currently used GSI, will be lowered the barrier of accessing DCIs using SLCS (e.g. Shibboleth credentials) and will enable the usage of EMI components and services with other security infrastructures such as Kerberos. The services that provide *short-lived credentials* will integrate the ability to issue Grid credentials based on a user's national or institutional authentication system. This will enable a user to use their familiar authentication system in a *single sign-on* manner to *create and receive or delegate Grid credentials to services*, easing access and removing the need for complicated key and certificate handling.

Short Lived Credential Service (SLCS) issues short-lived X.509 certificates based on authentication at a Shibboleth Identity Provider – thus linking AAI and Grid infrastructures X.509 certificate issuing process automated and invisible to the end-user. SLCS will be extended within EMI into a Security Token Service, capable of handling multiple security token types (X.509, SAML, Kerberos, ...

Security Assertion Markup Language (SAML) is a standard way to pass security information in a token. The middleware stacks currently have some form of SAML capability but will be made interoperable by using a common SAML profile. This common profile will be used by a service soon-to-be-common throughout the middleware stack, SAML-enabled VOMS (VOMS-SAML). In a harmonization step, UNICORE will phase out its VO management system, UVOS. The middleware will also converge on using a standard SAML library, openSAML2. Use will be made of previous collaborative work in that the OMII-Chemomentum (UNICORE) profile document is used as a starting point for the common SAML profile.

A *common set of authentication libraries* used by all the services in the middleware will provide a consistent set of authentication decisions throughout the middleware. Another consideration is the reduction in the amount of authentication code present and the increased ease of maintenance. These libraries will support standard methods such as TLS/SSLv3 with standard X.509 certificates and should extend to other standard methods such as HTTP authentication (username & password). This last point may be important for Grid communities that work via web access only.

Currently there are different authorization mechanisms used throughout the middleware. As harmonization and evolution steps within the middleware *a single authorization service that provides user-friendly features will be integrated throughout*--this is *Argus*, a site central service that can administer and enforce authorization policies in a hierarchical manner.

From the use-ability point of view, Argus provides users a means to create and administer XACML policies with a simplified language. In order to integrate this service, a common XACML profile is being created and introduced. Argus is compatible within the middleware by virtue of its standards adherence.

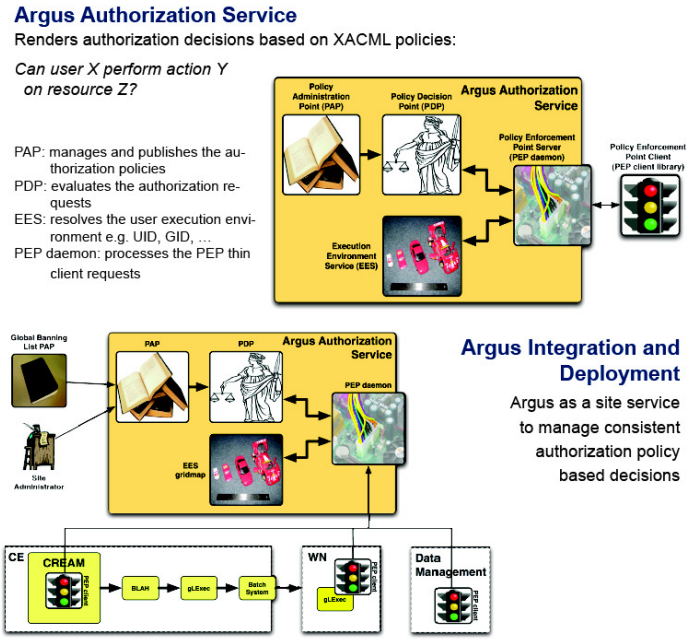


Fig. 9 – The Argus Authorization System.

10i) Operations

Not applicable.

(C11) The StratusLab OS Cloud Middleware Provider collaboration

Web Site: stratuslab.eu

Document repository: stratuslab.eu/doku.php/deliverables

Contact person: Charles Loomis (loomis@lal.in2p3.fr)

11a) Description of RI

StratusLab develops and provides a complete, open-source cloud distribution that allows resource centres to provide a private cloud infrastructure to their users and/or a public cloud infrastructure for external users. The primary use case for the project's cloud distribution involves running the grid services of the European Grid Infrastructure (EGI) within a private StratusLab cloud at each participating grid resource centre. Nonetheless, the distribution is more general and is perfectly adapted for providing private or public cloud infrastructures independent of EGI.

To validate the project's software, it operates a certified EGI grid site over a StratusLab cloud. It also provides a reference cloud infrastructure allowing interested scientists and system administrators to test the software and provide feedback. Although not permanent infrastructures, they do ensure that the StratusLab cloud distribution can meet the operational requirements of EGI and of resource centres.

11b) PA/NC collaboration explanation

StratusLab is a project co-funded by the European Commission through the FP7 Capacities program. Consequently, the European Commission as a public authority is directly implicated in financial cooperation with the project partners. Most of the partners (4 of 6) are public or quasi-public institutions that provide both financial and material support to the project.

All of the academic partners have strong links to their National Grid Initiative (NGI). Specifically, the NGIs for France, Greece, Spain, and Ireland are strongly linked to the project. Other NGIs have expressed interest in the project's software and it is expected that most NGIs will be involved directly or indirectly when grid resources centres begin adopting the StratusLab cloud distribution.

The StratusLab partners wish to continue the present collaboration after the formal end of the StratusLab project. The vehicle for this collaboration (another EC-funded project, memoranda of understanding between institutes, etc.) will depend on circumstances at the end of the current project, but the public authorities and national champions are likely to support the continued collaboration.

11c) Budget, funding model, economic sustainability

The total cost of the StratusLab project is approximately 3.2 M€ (2.3M€ EC-funding) over two years of which 3.0 M€ is used for non-management expenses. For the non-management expenses, approximately 52% is for integration and operation, 27% for dissemination and user support, and 21% for software development.

All of the partners are interested in using the StratusLab cloud distribution for their own purposes after the end of the project and have expressed a desire to continue their collaboration in some form. Presumably, the costs for the continued development will be borne at least partially by the current partners. Some of those costs could be shifted to users of the software distribution though support or service contracts, although concrete models for such a mechanism have not been discussed.

11d) Governance / Management

The StratusLab cloud distribution provides software appropriate for the deployment of both private and public clouds. The presumption is that these clouds are deployed by a single institute (or organization) and subject to its own governance and management policies.

The distribution, however, provides mechanisms by which resources can be federated (e.g. grid authentication/authorization mechanisms, shared machine/disk images through the StratusLab Marketplace, publishing accounting information to external servers, etc.). If a StratusLab is part of a federated infrastructure, then the governance and management policies of that federated infrastructure will have to be followed. StratusLab does not impose significant constraints on the possible governance and management models of the federated infrastructure. Specifically, the governance and management models used by EGI are entirely compatible with the StratusLab cloud distribution.

11e) Users and interaction model

The primary deployment model for StratusLab is the adoption of the project's software by the majority of sites involved in EGI. Sites run a StratusLab cloud on their physical hardware, run grid services within their cloud, and participate in EGI. As such, it is expected that all current EGI users will implicitly become users of StratusLab services through the grid services hosted on StratusLab clouds. Consequently, the number and scope of the current EGI users are a good first order estimate of the expected StratusLab user base.

Additionally, this deployment model allows sites to expose their resources also as a public cloud. The flexible, dynamic nature of these resources will attract a wider variety and larger number of scientists to EGI. The size of this additional user community has not yet been estimated, but is expected to be significant. Reasonable estimates can be made after the initial production release of the StratusLab cloud distribution (May 2011) when experience will be gained with production deployments and real scientific users.

11f) Countries and international collaborations

The countries involved directly in the project are: France, Greece, Ireland, Spain, and Switzerland. As the initial deployment targets are EGI sites, it is expected that most countries involved in EGI will also collaborate directly or indirectly with the project. There has been explicit interest from several National Grid Initiatives for running cloud infrastructures with the StratusLab software. Interest has been shown from institutes in Vietnam.

11g) History and evolution

Most (five of six partners) had already started collaborating on cloud technologies before the FP7 StratusLab project was conceived and accepted. This collaboration grew out of work started within the EGEE series of projects. Two components reused by the StratusLab cloud distribution are OpenNebula (developed by UCM) and Claudia (developed by Telefónica I+D). Both of these were developed within the context of the Reservoir project. The project's detailed program of work grew out of partner experiences in the above project but also experience with Amazon's cloud services, Eucalyptus, VMware, VirtualBox, and other cloud and virtualization technologies.

11h) Security

The project supports a wide range of different authentication mechanisms, including simple username/password pairs, LDAP authentication, grid certificates, and VOMS proxies. Once authenticated all rights (permissions) are currently managed solely on the user's identity. The first production release (May 2011) is expected to allow authorization based on group and role information as well.

The StratusLab Marketplace stores cryptographically signed metadata concerning shared machine and disk images. Cloud administrators can define trust policies for authorizing (or not) certain machine or disk images to be used on their infrastructure. Owners of the images control the storage of the actual images and thus access to them.

StratusLab has already enhanced the available logging information and implemented a quarantine feature specifically to facilitate forensic analysis should security problems arise. Eventually, it will also suggest additional tools to monitor in "real-time" the activity of running virtual machines (esp. network activity).

The security policies are expected to closely mirror those already in place at the cloud administrator's institute for individual private or public cloud deployments. If the cloud is part of a larger distributed computing infrastructure (such as EGI), then the cloud policies are expected to mirror those policies.

11i) Operations

StratusLab provides an "Infrastructure as a Service" cloud, meaning that operations of services are very similar whether on physical or virtual nodes. However, the ability to migrate services easily from failing hardware or for load balancing should simplify normal service management tasks. Given that the operations tasks are very similar to those for physical hardware, the StratusLab cloud distribution should not perturb any existing operations policies or procedures.

(C12) The Venus-C Public/Private Cloud M.Ware Provider collaboration

Web Site / Document repository / Wiki: www.venus-c.eu

Contractual documents:

Contact person: Andrea Manieri

12a) Description of RI

Cloud computing can transform the way research is conducted by empowering the research community broadly in new ways, ultimately accelerating global scientific exploration,

discovery and results. VENUS-C (*Virtual multidisciplinary EnviroNments USing Cloud Infrastructures*) is a pioneering project for the European Commission's 7th Framework Programme that draws its strength from a joint co-operation bringing together industrial partners and scientific user communities. Its aim is to develop and deploy a Cloud computing service for research and industry communities in Europe by offering an industrial-quality, service-oriented platform based on virtualisation technologies facilitating a range of research fields through easy deployment of end-user services. Current user communities involved are: bioinformatics, systems biology, drug discovery, civil engineering, civil protection and emergencies and data for science. The Open Call, which will be launched in early January 2011, aims to extend the current user scenario portfolio and enable a new generation of research applications to validate the infrastructure for advancing scientific discovery.

The VENUS-C solution is an open and generic *Application Programming Interface* (API) at platform level for scientific applications, striving towards interoperable services.

The VENUS-C platform will be based on both commercial and open source solutions underpinned by the Engineering data centre, Microsoft through Windows Azure and its European data centres, along with two European High Performance Computing centres: The Royal Institute of Technology (KTH, Sweden) and the Barcelona Supercomputing Centre (BSC, Spain). Azure offers a multi-layer solution, including computing and storage power, a development environment and immediate services, together with a wide range of services that can be consumed from either on-premises environments or the Internet. From an Open Source perspective, the Eucalyptus and OpenNebula solutions are being evaluated, while the EMOTIVE middleware for clouds will be offered by the Barcelona Supercomputing Centre, thus demonstrating interoperability and ultimately portability to VENUS-C users.

12b) PA/NC collaboration explanation

VENUS-C currently has seven user scenarios, including the National Research Council of Italy, which focuses on marine biodiversity data needed by international organizations such as FAO. The scenario for Civil Protection and Emergencies targets public authorities such as civil protection agencies.

12c) Budget, funding model, economic sustainability

VENUS-C is co-funded by the GÉANT and e-Infrastructure Unit, DG Information Society and Media of the European Commission, as one of six European *Distributed Computing Infrastructures* (DCIs). VENUS-C is committed to working in synergy with these initiatives, combining experiences in Grid infrastructures and Cloud computing to capitalize on EU investments. VENUS-C brings together 14 European partners. Industry funding stems from Microsoft Redmond, which invests in manpower and Azure resources, as well as its data centres. The Engineering Group (Italy) will also provide support through its data centre. The total budget is €8,803,064 with funding from the EC of €4,500,000. The budget for the Open Call is €400,000, which will be equally distributed to the new pilots in addition to compute resources (Azure, Royal Institute of Technology and the Barcelona Supercomputing Centre), technical support and training.

A specific task in VENUS-C is dedicated to investigating the legal issues associated with scientific cloud computing, business models and sustainability.

12d) Governance / Management

The current governance and management model is through the funding scheme described above. Sustainability studies will investigate the potential for longer term business and governance models serving Europe's small business and scientific communities.

12e) Users and interaction model

Collectively, the current seven scenarios have potential benefits across a variety of thematic areas: *Civil Engineering*, *Civil Protection and Emergencies*, *Biomedicine* and *Marine Biodiversity* data. Part of the selection criteria for the Open Call includes the potential user base of selected pilots. Part of the sustainability work will focus on potential services to target communities. All end-users, including the successful new pilots, are provided with continuous technical support and training, fostering close partner interaction.

12f) Countries and international collaborations

The VENUS-C consortium includes 14 partners from Germany (1 partner), Greece (2 partners), Israel (1 partner), Italy (4 partners), Spain (2 partners), Sweden (1 partner) and the UK (3 partners). VENUS-C co-operates with the six European DCIs based on a pre-defined work plan and formalized through a Joint Cooperation Report (September 2010). VENUS-C is committed to ensuring active participation in EGI technical and user forums, as well as *e-Infrastructure Concertation Meetings*.

VENUS-C works closely with SIENA (Standards and Interoperability for eInfrastructure Implementation Initiative) on standards, contributing to the SIENA Roadmap dedicated to Grids and Clouds Standards for eScience and Beyond) in synergy with international standards groups (OGF, SNIA, OASIS, DMTF, ETSI, NIST) and the other DCIs. Microsoft is participating in four use case projects spearheaded by standards groups (DMTF Cloud Working Group, NIST, ISO/JTC1 SC38 Cloud Computing, Fraunhofer/FOKUS). VENUS-C also interacts with policy bodies (e-IRG, ESFRI). VENUS-C Director, Andrea Manieri, has worked with ENISA as a security expert with regard to a Cloud computing assurance framework. VENUS-C has developed a synergy with e-ScienceTalk to support dissemination activities. Additional synergies will be established through the life-time of VENUS-C in keeping with the project's goals.

VENUS-C co-ordinates an External International Advisory Committee (EIAC) with three members from the U.S. and two from Europe to shape the strategic direction of the project and support the evaluation of the Open Call. An IT legal expert has been recruited to support the project's investigation into legal issues, bringing insights also from collaboration with ENISA.

12g) History and evolution

VENUS-C partners have experience of Grid computing since the early days (Project Chair served as Director of DataGrid), with several partners continuing involvement in the three phases of EGEE, as well as related projects such as EUIndiaGrid, EUMEDGRID and EUMEDGRID-Support, D4Science. However, several partners are new to distributed computing (3D rendering – civil engineering application, virtual fire – civil protection, drug

discovery and systems biology – biomedicine). VENUS-C grew out of a recognized need to foster the easy deployment of end-user services to Europe's small business and scientific communities by developing and testing the foreseen platform.

12h) Security

Regarding application security a set of technologies and standards around federated authentication and authorization has been selected as being relevant to VENUS-C to support state of the art and platform independent claims based authentication and authorization services. Currently, the following technologies are of relevance to VENUS-C from an application security perspective: SAML Tokens, WS-Trust, WS-Foundation, ADFS. The VENUS-C Architecture Report details how cross-cutting concerns such as security, accounting, billing, and networking are addressed.

Property rights are governed by the Consortium Agreement. The property rights of the new pilots recruited through the Open Call will be unaffected in that successful candidates will retain intellectual property.

12i) Operations

The VENUS-C solution is an Open and generic *Application Programming Interface* (API) at platform level for scientific applications, striving towards interoperable services. The VENUS-C platform will be based on both commercial and open source solutions underpinned by the Engineering data centre, Microsoft through the Windows Azure and its European data centres, and two European High Performance Computing centres: The Royal Institute of Technology (KTH, Sweden) and the Barcelona Supercomputing Centre (BSC, Spain). Azure offers a multi-layer solution, including computing and storage power, a development environment and immediate services, together with a wide range of services that can be consumed from either on-premises environments or the Internet. From an Open Source perspective, the Eucalyptus and OpenNebula solutions will be evaluated, while the Emotive middleware for clouds will be offered by the Barcelona Supercomputing Centre, thus demonstrating interoperability and ultimately portability to the VENUS-C users.

Technical challenges addressed include virtualisation, service orientation and digital convergence, which are at the heart of the cloud model, as well as current open issues on interoperability with existing DCIs (e.g. Supercomputers), *Data Management*, *Programming Models*, *Application Security*, *Monitoring and Accounting*, *Networking and Network Security*.

In the first twelve months, the project will focus on the delivery of an end-to-end prototype which delivers immediate value to scientific partners: the first release will focus on dynamic job submission and workload dispatch into multiple underlying DCI and cloud providers. Subsequent milestones will enable integration with data management, security and programming models, working in synergy with our scientific users, primarily focusing on the functionality of directly usable application-level. Less-visible infrastructure work will start after the initial delivery of the core platform.

2.4 Virtual Research Community (VRC) Collaboration

(C13) The WLCG HEP Physics VRC

Web Site / Document repository / Wiki: www.cern.ch/lcg

Contractual documents: MoU[11] and Annexes

Contact person: lcg.office@cern.ch

13a) Description of RI

The *Worldwide LHC Computing Grid* (WLCG) is the world's largest computing grid, as it links grid infrastructures and computer centres worldwide. It is the outcome of a global collaboration of more than 140 computing centres in 34 countries, the four experiments at the *Large Hadron Collider* (LHC), and several national and international grid projects. The mission of the WLCG project is to build and maintain a data storage and analysis infrastructure for the entire high energy physics community that will use the Large Hadron Collider at CERN. It was launched in 2002 to provide global computing resource to store, distribute and analyse the 15 Petabytes (15 million Gigabytes) of data annually generated by LHC.

13b) PA/NC collaboration explanation

WLGC is a collaboration between the LHC experiments and worldwide computing centres.

13c) Budget, funding model, economic sustainability

It is funded by the same funding agencies that support LHC experiments, i.e. CERN international laboratory and many national agencies. Each year the planning is based on the basis of pledged compute and storage resources for the following five years.

13d) Governance / Management

The *Collaboration Board* (CB) provides the main technical direction for LCG. The CB is composed of a representative of each Institution or federation of Institutions that is a member of the Collaboration, the LCG *Project Leader* and the *Spokespersons* of each LHC Experiment, with voting rights; and the CERN *Chief Scientific Officer* (CSO), and CERN/IT and CERN/PH *Department Heads*, as ex-officio members without voting rights, as well as a Scientific Secretary.

[11] See: lcg.web.cern.ch/LCG/MoU/Brazil/MoU-Brazil-CERN-20Apr09.pdf.

A standing committee of the CB, the *Overview Board* (OB), has the role of overseeing the functioning of the Collaboration. The *Management Board* (MB) supervises the work of the Project.

13e) Users and interaction model

The *Grid Deployment Board* (GDB) is the forum within the Project where the computing managements of the experiments and the regional computing centres discuss and take, or prepare, the decisions necessary for planning, deploying, and operating the LHC Computing Grid. Its membership includes: as voting members – one person from each country with a regional computing centre providing resources to an LHC experiment (usually a senior manager from the largest such centre in the country), a representative of each of the experiments; as non-voting members – the *Computing Co-ordinators* of the experiments, the LCG *Project Leader*, and leaders of formal activities and projects of the Collaboration.

13f) Countries and international collaborations

Australia, Austria, Belgium, Brazil, Canada, China, Czech Republic, Estonia, Finland, France, Germany, Hungary, India, Israel, Italy, Korea, Netherlands, Norway, Pakistan, Poland, Portugal, Romania, Russian Federation, Slovenia, Spain, Switzerland, Sweden, Taiwan, Turkey, United Kingdom, Ukraine, United States.

WLCG relies on both EGI infrastructure in Europe and OSG infrastructure in the US.

13g) History and evolution

WLGC dates back to 2002 and its history is marked by a rapid evolution over time, which reflects a long series of successful challenges on data access and distribution, before the beginning of LHC data taking. The TDR has been signed in 2005. The increase of resources available to WLCG is compatible with the gathering of LHC data, at a rate of about 15 PB/year.

13h) Security

The *Grid Security Infrastructure* (GSI) in WLCG enables secure authentication and communication over an open network. GSI is based on public key encryption, X.509 certificates, and the *Secure Sockets Layer* (SSL) communication protocol, with extensions for single sign-on and delegation. In order to authenticate himself, a user needs to have a digital X.509 certificate issued by a *Certification Authority* (CA) trusted by the infrastructure running the middleware.

The authorisation of a user on a specific Grid resource can be done in two different ways. The first is simpler, and relies on the grid-mapfile mechanism. The second relies on the *Virtual Organisation Membership Service* (VOMS) and the LCAS/LCMAPS mechanism, which allow for a more detailed definition of user privileges.

13i) Operations

Since the start of LHC data taking, the WLCG collaboration is running more than 1,000,000 tasks per day on 200,000 processors from 140 computing centres in 40 countries, as well as multi GB/s data transfer on the full mesh of its tiered centres. WLCG operations rely on the *European Grid Infrastructure* (EGI) in Europe and the *Open Science Grid* (OSG) in the US.

(C14) The WeNMR VRC

Web Site / Document repository / Wiki: www.wenmr.eu

Contractual documents: e-NMR Grant Agreement n.213010 - Annex DoW; We-NMR Grant Agreement n.261572 - Annex DoW Memorandum of Understanding between EGI.eu and WeNMR VRC (DRAFT)

Contact person: Alexandre M.J.J Bonvin

14a) Description of RI

The WeNMR VRC aims at bringing together complementary research teams in the structural biology and life science areas into a virtual research community at a worldwide level, with an initial focus on the biomolecular *Nuclear Magnetic Resonance* (NMR) and *Small Angle X-ray*

Scattering (SAXS) communities. Challenges in the post-genomic era, like the analysis of biomolecular interactions, call for European and worldwide interdisciplinary collaborations that are hardly imaginable without embracing the e-Science paradigms. This research needs virtual research platforms that provide the worldwide life science research community with user-friendly computation tools, platforms for data analysis and exchange, e-Science tools for conferencing, exchange of best practice and training, all supported by an underlying high performance e-Infrastructure. The WeNMR project (contract RI-261571), funded under the FP7 e-Infrastructure Virtual Research Community call, builds upon the established FP7 I3 eNMR three years e-Infrastructure project (grant no. 213010). Its steadily growing WeNMR.eu *Virtual Organization* (VO) is currently the second largest in the life science area with 235 members to date, over 10% of which are outside Europe.
The main objective of WeNMR is to establish an e-Infrastructure-based global virtual research community for structural biology in the life sciences. To this end six objectives are defined: (1) to operate, maintain and further develop *a user-friendly science gateway* for the NMR and SAXS communities, (2) to establish *a virtual research platform* to serve as a digital knowledge repository, data exchange medium, and forum for (interaction with) the user community, (3) to *provide support to software developers, users and other e-Infrastructure projects* in an e-Science knowledge and training centre, (4) to *foster the adoption and use of e-Infrastructure on a global scale* by supporting a wide range of flanking disciplines within the life sciences, (5) to *operate and consolidate the eNMR Grid infrastructure* in line with NGIs and the EGI, and to extend it to interoperate with other worldwide Grid initiatives, (6) to develop a model to *ensure sustainability of the project*.

The partners in the WeNMR project are represented indirectly in the EGI Council through their NGIs.

14b) PA/NC collaboration explanation

This VRC is composed of public academic and research institutions, represented by the NGIs.

14c) Budget, funding model, economic sustainability

The WeNMR VRC is based on the WeNMR Project funded by the EC. The expected total costs are 2,433,988.00 Euros, and the requested EU Contribution 2,150,000.00 Euros.

Regarding the collaboration with EGI.eu, each Party shall bear the costs of discharging its respective responsibilities under this MoU, including travel and subsistence of its own personnel and transportation of goods and equipment and associated documentation, unless otherwise agreed in the MoU. Each Party shall make available free of charge to the other Party any office/meeting space needed for the joint activities. The Parties' obligations are subject to their respective funding procedures and the availability of appropriated funds. Should either Party encounter budgetary problems in the course of its respective internal procedures that may affect the activities carried out under this MoU that Party shall notify and consult with the other Party in a timely manner in order to minimise the negative impact of such problems on the cooperation. The Parties shall jointly look for mutually agreeable solutions.

14d) Governance / Management

The term *Virtual Research Community* (VRC) refers to an organisational grouping that brings together transient Virtual Organisations within a persistent and sustainable structure. A VRC is a self-organising group that collects and represents the interests of a focussed collection of researchers across a clear and well-defined field. Named contacts are agreed upon by the VRC to perform specific roles and these then form the communication channel between the VRC and EGI.eu.

14e) Users and interaction model

The interest of the user community for this kind of services is well reflected in the growth of the WeNMR.eu VO over the last year, which has now reached 135 registered members, both from within and outside (12) Europe (see Fig. 10), making it the second largest VO in the Life Sciences. This growth is observed despite the fact that many of the tools have only very recently been made available.

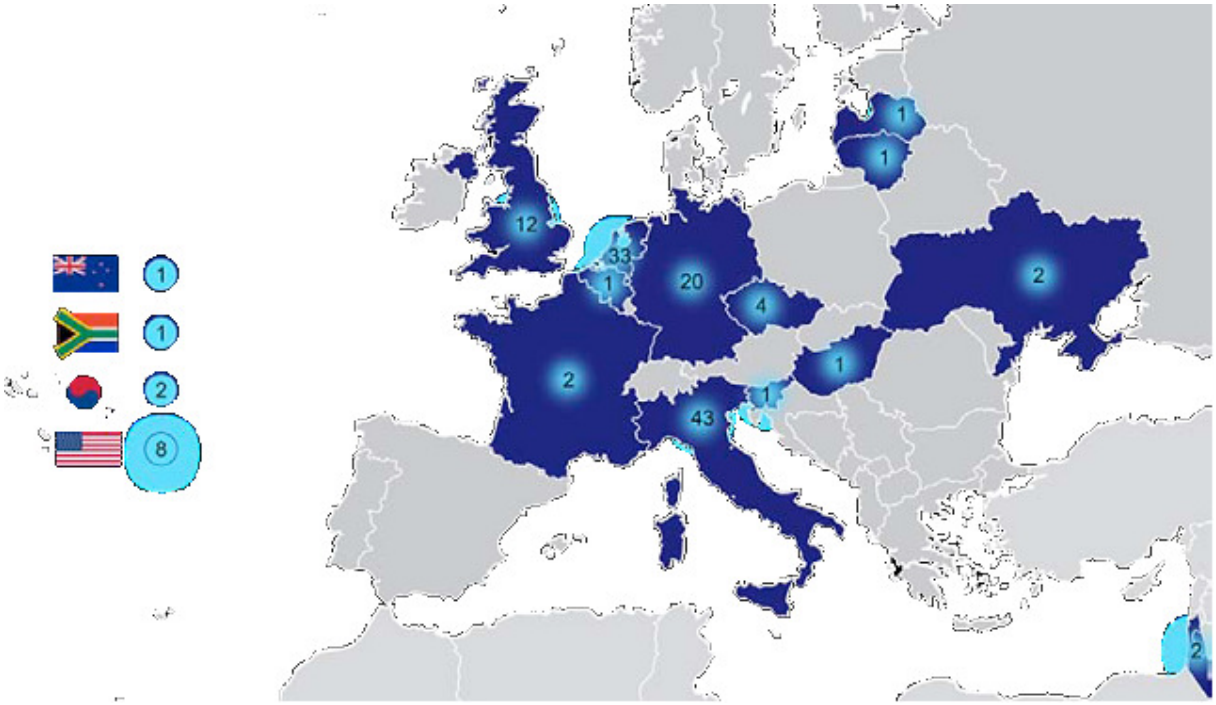


Fig. 10 – Geographical view of e-NMR users' distribution.

14f) Countries and international collaborations

The goal of the collaboration defined by the MoU between WeNMR and EGI.eu is to establish a formal relationship. The WeNMR resource centres will be integrated with EGI through the respective National Grid Initiatives once they reach EGI production-quality. EGI and the relevant NGIs will jointly deliver the operational and user support services needed to make the WeNMR resources seamlessly, reliably and securely accessible to the relevant user

communities. As regards the user community around WeNMR, the project will bring them together as an emerging VRC in the area of structural biology and life sciences.

The objectives of the collaboration are:

- *user support*,
- *application integration*,
- *user community policy and procedures*,
- *requirements gathering*,
- *sustainability*,
- *dissemination*.

The countries involved in WeNMR are The Netherlands, Germany, Italy, UK, Lithuania.

14g) History and evolution

14h) Security

The synchrotron SAXS instrument X33 of the EMBL Hamburg has recently been equipped with a robotic sample changer and the beamline meta server software, allowing for fully automated and remote operation by users sending in 96-well plates. The new high brilliance BioSAXS beamline of the EMBL at the storage ring Petra-III in Hamburg (currently under construction, to be operational in 2010) will make full use of automated and remote data collection options. Presently, the remote access to X33 is achieved using a NoMachine client-server protocol.

The access to remote SAXS instrumentation will make the actual SAXS experiments possible for individual users, without the need for the actual physical presence of the experimenter at the EMBL Hamburg location. Users can send in samples in 96-well plates that can be measured at the Hamburg X33 synchrotron SAXS instrument in fully automated mode or by remote operation. Implementing a secure, grid-enabled gateway will significantly enhance both efficiency and security of remote access to the biological SAXS instruments.

A possible solution for the gateway will be the technology developed for the Instrument Element (IE). The IE is a concept developed initially by GRIDCC, a FP6 project coordinated by INFN. It is an abstraction of the instrument (or group of instruments) into a standard interface, which can be used within the rest of the GRIDCC architecture. The term instrument is used in this context to define a piece of equipment that needs to be initialized, configured, operated (start, stop, standby, resume, application specific commands), monitored or reset. The current version of the IE has been further developed by the FP7 DORII project, and is now a set of WS-I compliant web services virtualising the concept of instrument and sensor and presenting this as a grid component compatible with the gLite middleware. IE has been endorsed by the RESPECT program[12], so it could be a good candidate to provide components on top of which to build a scientific gateway, fully compatible with the WeNMR grid infrastructure, for enabling complex workflows including secure remote access to SAXS instrumentation.

[12] *Recommended External Software for EGEE CommuniTies*, see: technical.eu-egee.org/index.php?id=290.

14i) Operations

The WeNMR Project WP4 aims at continuing and improving the operation of the Grid infrastructure and of the services that were developed within the e-NMR project. This will occur both at the level of the infrastructure itself, i.e. by ensuring software and hardware updates and at the level of the interaction with users. WP4 will operate the scientific gateway for the various web-based tools that WeNMR will offer to its users and add new Grid-enabled web portals to it. The gateway will be extended as required to meet the specific needs of WeNMR users and other stakeholders, such as software developers willing to contribute additional tools to the portfolio of WeNMR.

To facilitate both Grid administration and maintenance and end-user interaction with the WeNMR services, virtual machines will be made available. Secured and web accessible workspaces and data storage will be implemented.

Objectives:

- maintaining the operation of the GRID infrastructure, introducing all relevant software and hardware upgrades,
- installing, maintaining operational and improving the WeNMR Gateway,
- identifying and providing services that respond specifically to the needs of members of the WeNMR.eu VO.

3. The (HPC) Top Parallel Computing RI Ecosystem

3.1 Tier-0 Capability Computing Centres Collaborations

No Tier-0 Capability HPC centres collaborations were surveyed.

3.2 Tier-1 National and Regional Computing Collaborations

(C15) The Netherlands Computing Facilities Foundation (NCF)

Web Site / Document repository / Wiki: www.nwo.nl/ncf

Contractual documents:

Contact person: Patrick Aerts (Director)

15a) Description of RI

The Netherlands *National Computing Facilities* foundation (NCF) is an independent foundation under the umbrella of the *Netherlands Organisation for Scientific Research* (NWO). NCF is responsible for the high-end computing infrastructure for science and research in the Netherlands.

NCF conducts the following activities:

- formulate and realise a long term policy for advanced computer infrastructure for scientific research in the Netherlands, in the European context;
- set the Dutch national high-end computer agenda, working in close co-operation with research councils, user groups, high-performance computing centres and universities;

- assessment of scientific computing requirements, issuing Request for Proposals, process procurements, pro-active benchmarking of systems;
- acquisition of state-of-the-art supercomputer systems;
- develop together with Nikhef (*National Institute for Subatomic Physics*) and NBIC (*National Bioinformatics Centre*) the nation-wide Science Grid in the Netherlands (BiG Grid);
- act as the Dutch National Grid Initiative (NGI) which participates in the pan-European EGI Grid Initiative;
- participate in European and global e-infrastructure projects;
- support initiatives of Dutch universities and/or research institutes to locally install medium-range high-performance computing facilities, also financially, provided that the system to be installed will be made available nationwide through NCF. In this way, NCF tries to maintain a coherent national computer infrastructure;
- keep and maintain a database on European national policies in HPC and grids, HPC-resources (computing systems) and a database on commercially available supercomputers;
- keep and maintain the e-IRG knowledge base[13].

The central components of the Research Infrastructure provided by NCF are:

- the national supercomputer (Huygens), a 3,328 core IBM Power 575 Hydro-Cluster with a peak performance of 60 TFlop/s, 15,616 GB memory and 972 TB disk capacity,
- the national computer cluster (Lisa), with 4,480 cores and 12 TB memory, [14]
- the national Grid Infrastructure (BiG Grid) with 7,000 cores and 7,000 TB storage.

15b) PA/NC collaboration explanation

NCF is part of the *Netherlands Organisation for Scientific Research* (NWO). NWO stimulates and finances research in every conceivable scientific discipline and facilitates innovations. NWO is autonomous but falls under the responsibility of the Ministry of Education, Culture and Research.

15c) Budget, funding model, economic sustainability

NCF's budget for 2011 is € 15.4 million. The structural component of the budget, which is provided by NWO, is € 6.8 million. The size of the variable component depends on the projects being carried out. A proposal for sustainable funding for all components of the Dutch high-end ICT infrastructure for scientific research has been approved by the (previous) government but waits for final decisions of the current government on the funding model and level.

[13] See: knowledgebase.e-irg.eu.
[14] Lisa is co-funded by NCF, the *University of Amsterdam* (UvA), the *Free University of Amsterdam* (VU), the foundation *Netherlands Bioinformatics Centre* (NBIC) and the NWO Program *Computational Life Sciences* (CLS).

15d) Governance / Management

The *Board of Directors* of NCF is appointed by NWO and consists of four high-ranking members from universities, typically university board members, and one representative from the industrial R&D community. Within the organization of NWO, NCF reports directly to the General Board of NWO. A *Committee for Scientific Use of Supercomputers* (WGS) consisting of eight members of the academic community and a representative from industrial R&D advises the Board of Directors on policy issues.

The NCF Bureau is led by a Director and has eleven staff members (7.3 FTE).

15e) Users and interaction model

All researchers at universities and academic research organisations can apply for resources on the national supercomputer, the national cluster, the grid infrastructure or for other grants, e.g. for the parallelisation of codes. The *Committee for Scientific Use of Supercomputers* (WGS) is in charge of peer review of these user proposals and for the allocation of these resources.

15f) Countries and international collaborations

NCF participates in the following international initiatives and projects:

- PRACE (*Partnership for Advanced Computing in Europe*). The Huygens system is part of the DEISA supercomputing grid which is now being integrated in the PRACE RI,
- EGI (*European Grid Initiative*). Big Grid is part of the European Grid Infrastructure,
- EEF (*European e-Infrastructures Forum*),
- IESP (*International Exascale Software Project*),
- EESI (*European Exascale Software Initiative*),
- OSIRIS (*towards an Open and Sustainable ICT Research Infrastructure Strategy*),
- e-IRG (*e-Infrastructures Refection Group*) and e-IRGSP3 project (*e-IRG support programme*).

15g) History and evolution

The first national supercomputer facility (a Cyber CDC 205) was installed in 1984. Since then the national facility has been replaced approximately every six years. NCF was founded in 1990.

15h) Security

Security is taken care of by the operators of the resources (see next item).

15i) Operations

The operation of the national systems is outsourced to SARA (Huygens, Lisa and BiG Grid) and to Nikhef (Big Grid).

(C16) Finland CSC HPC Centre

Web Site / Document repository / Wiki: www.csc.fi

Contractual documents:

Contact person: Ignatius Janne (Director Computing)

16a) Description of RI

The Finnish academic supercomputing policy is defined by the Ministry of Education and Culture which also provides the funding for the supercomputer facilities. Research institutes which are under other ministries have their own sources of funding.

CSC – IT Centre for Science Ltd (CSC) is the national organization responsible for academic supercomputing, research networking, data storage and scientific software and database services. It is a non-profit company whose shareholder is the Ministry of Education and Culture.

The supercomputer systems provided by CSC are:

- Cray XT4/XT5 (Louhi) with a total of 10,684 cores and 11.7 TB memory. The peak performance is 102.3 Tflop/s;
- HP CP4000 BL Proliant supercluster (Vuori) with a total of 2,880 cores and 5,722 GB memory. The peak performance is 30 Tflop/s;
- HP CP4000 BL Proliant supercluster (Murska) with 2,176 cores and 5,120 GB memory. The peak performance is 11.3 Tflop/s;
- M-grid (Material Sciences Grid), the National Grid Initiative of Finland. The participants are CSC, Tampere University of Technology, University of Helsinki, Helsinki University of Technology, University of Jyväskylä, Lappeenranta University of Technology, Turku University and Helsinki Institute of Physics.

16b) PA/NC collaboration explanation

CSC is administered by the Ministry of Education and Culture.

16c) Budget, funding model, economic sustainability

The budget of CSC in 2010 was € 25.6 million.

16d) Governance / Management

CSC's statutory bodies are the *General Meeting of Shareholders*, the *Board of Directors* and the *Managing Director*. The *Annual General Meeting* (AGM) is the highest decision-making organ of CSC. The Board of Directors of CSC has four to seven representatives from the Ministry of Education and Culture, academia, and related institutes which are elected by the AGM. The Board of Directors appoints the Managing Director who together with the Management Group is responsible for the operative management.

16e) Users and interaction model

In 2010 the HPC facilities were used by all Finnish universities, five universities of Applied Sciences, the Finnish Meteorological Institute and industry. International users were granted access through the DEISA, EGI and HPC-Europe2 projects or other collaborations.

The basic principles and priorities of resource allocations are defined by CSC's Board of Directors. The national HPC resources are allocated by the CSC Resource Allocation Group which accepts applications for national HPC resources continuously. In addition, Grand Challenge proposal calls are opened twice a year. These proposals go through a technical and a scientific evaluation. The scientific evaluation of these proposals is done with the help of CSC's Computational Services Customer Panel, comprised of Finnish research group leaders in several scientific disciplines. All applications and proposals are measured by their scientific effectiveness and quality. The use of the HPC resources is free of charge for Finnish university and polytechnic researchers.

16f) Countries and international collaborations

CSC participates in several international supercomputing and grid infrastructure development projects. Examples of international collaboration are:

- PRACE (*Partnership for Advanced Computing in Europe*). CSC participates in the PRACE Association and in the PRACE project;
- DEISA (European HPC grid). CSC is one of the participating HPC centres;
- EGI (*European Grid Infrastructure*);
- HPC-Europa2, a project supporting mobility of European researchers between HPC centres;
- EUFORIA (*EUropean initiative FOR Iter Applications*), a project that modelled European Tokamak reactors.

CSC also participates in several ESFRI projects and other FP7 funded projects.
Foreign researchers can use CSC's computing facilities. In 2010 the total number of foreign accounts was 887.

16g) History and evolution

The first Finnish national computer system, a Univac 1108, was installed in 1971 at the Finnish State Computer Centre. At that time a new Operational Unit 2 (KT2) was established

which in time became CSC. The first real supercomputer, a Cray XMP, was installed at CSC in 1989. Since then several new installations have taken place.

In 2010 CSC decided to establish an eco-efficient (near zero carbon footprint) HPC centre in Kajaani, in Northern Finland. This data centre is being built in an old paper mill which has three hydropower stations on site. The government granted € 25 million funding for this data centre.

16h) Security

CSC's operations and services adhere to recommended security practices.

16i) Operations

CSC employs 210 staff members.

3.3 The PRACE Collaboration

(C17) The PRACE/DEISA HPC Centres Collaboration

Web Site / Document repository / Wiki: www.prace-project.eu , www.deisa.eu

Contractual documents: Statutes of the PRACE AISBL

Contact person: Thomas Eickermann (PRACE), Hermann Lederer (DEISA)

17a) Description of RI

PRACE, the *Partnership for Advanced Computing in Europe*, is a persistent pan-European High Performance Computing Service. The PRACE Research Infrastructure consists of several supercomputers in the Petaflop/s range. PRACE aims to maintain up to six world-class systems (so called Tier-0 systems) well integrated into the European HPC ecosystem. Each system will provide computing power of several Petaflop/s in midterm and on the longer term (2019) in the Exaflop/s range. The current systems are an IBM BlueGene/P at Forschungszentrum Jülich, Germany (JUGENE, 1 Petaflop/s) and a Bull at CEA, France (CURIE, 1.6 Petaflop/s when the last phase of the installation will be completed in October 2011). A third system, a Cray XE6 at the Computing Centre of the University of Stuttgart (HERMIT, 1 Petaflop/s) will be installed in the autumn of 2011. Also an IBM at Leibniz Rechenzentrum, Münich (SuperMUC, 3 Petaflop/s) will become operational in 2012.

DEISA, the *Distributed European Infrastructure for Supercomputing Applications*, is a consortium of eleven National Supercomputing Centres. DEISA provides a heterogeneous HPC infrastructure consisting of the systems at these centres (so called Tier-1 systems) tightly

interconnected through a dedicated high performance network (10 Gbps lines provided by GÉANT and the NRENs). The DEISA computer resources include several platforms and operating environments: Cray XT5 (Linux), Intel Xeon Nehalem (Linux), IBM Power6 (AIX, Linux), IBM BlueGene/P (Linux), IBM PowerPC (Linux), SGI ALTIX 4700 (Linux) and NEC SX-9 vector systems (Super UX). The aggregated power of the DEISA supercomputing resources exceeds two Petaflop/s.

It is the aim to integrate in the very near future the PRACE and DEISA HPC infrastructures into the European HPC ecosystem. A project proposal for the second implementation phase (PRACE-2IP) has been submitted to the EC and one of its objectives is this integration.

17b) PA/NC collaboration explanation

PRACE is a cooperation of 21 partner institutions of 21 European countries. Most of them represent the national HPC service providers. DEISA is a collaboration of 11 national HPC centres (the principal partners) in 7 European countries.

17c) Budget, funding model, economic sustainability

In PRACE each of four countries (France, Germany, Italy and Spain which are called the hosting partners) has given the commitment to provide 100 M€ in the next five years. This funding is complemented by up to 70 M€ from the European Commission as matching funds for the preparation and implementation of the PRACE Research Infrastructure. The budget for the current PRACE-1IP project is 28 M€ (20 M€ funded by the EC).

The budget of the DEISA2 project is 18.7 M€.

17d) Governance / Management

The PRACE RI is an international non-profit association named “Partnership for Advanced Computing in Europe AISBL”. It was created on April 23, 2010 by 19 members, representing Austria, Bulgaria, Cyprus, Czech Republic, Finland, France, Germany, Greece, Ireland, Italy, The Netherlands, Norway, Poland, Portugal, Serbia, Spain, Sweden, Switzerland, Turkey and the UK. Additional European states are invited to join. The seat of the PRACE AISBL is in Brussels.
PRACE AISBL has two bodies: the Council and the Board of Directors. The Council is the governing body and is composed of all members. The Council is led by a Board elected by the Council. The Board of Directors is the executive body of the Association and is composed of a minimum of two members, elected by the Council.

The governance of the PRACE-1IP project consists of:

- a *Project Management Board* as top-level decision taking and executive body in which all partners and the Director of the PRACE RI participate,
- a *Technical Board* consisting of the Work Package leaders and the Project manager which ensures coherence of the project,
- a *Project Manager* and *Project office* responsible for the execution of the project plan.

The governance of the DEISA2 project consists of:

- a DEISA *Executive Committee* as highest decision taking body with representatives of all principal partners with full voting rights and one representative of the associate partners,
- an *Extended* DEISA *Executive Committee* in which principal and associate partners participate and which acts as advisory board,
- a *Technical Board* consisting of the Work Package leaders and the Project Coordinator which ensures proper performance of the project,
- an *Advisory Scientific Committee* acting as external consulting board on scientific issues
- a *Project Coordinator* responsible for the execution of the project plan,
- a *Project Management Team* that supports the Project Coordinator,
- a *Technical Coordinator* responsible for the proper performance of the technical implementation of the project,
- a *Quality Assurance Coordinator*.

17e) Users and interaction model

The PRACE RI is accessible to applicants who have submitted a a successful proposal in response to Calls for Proposals. The proposals are subject to a peer review process which consists of a technical and a scientific assessment.

The DEISA resources are accessible for users who have submitted a successful proposal in response to a yearly Call for Proposals. The proposals were evaluated by national evaluation committees and the DEISA Executive Committee decided on the allocation based on the national recommendations.

Both PRACE and DEISA have experts who provide support and training to the users in porting, scaling and optimising their applications.

17f) Countries and international collaborations

The current 21 **PRACE partners** are: Austria (JKU - University Linz, Institute for Computer Architecture), Bulgaria (NCSA - Executive agency "Electronic communication networks and information systems"), Cyprus (CaSToRC - Computation-based Science and Technology Research Centre), Czech Republic (VŠB - Technical University of Ostrava), Finland (CSC – IT Centre for Science), France (GENCI – Grand Equipement national pour le Calcul Intensif), Germany (GCS – GAUSS Centre for Supercomputing), Greece: GRNET (Greek Research and Technology Network), Ireland (ICHEC - Irish Centre for High-End Computing), Italy (CINECA - Consorzio Interuniversitario), The Netherlands (NCF – Netherlands Computing Facilities Foundation), Norway (SIGMA - UNINETT Sigma AS - The Norwegian Metacenter for Computational Science), Poland (PSNC – Poznan Supercomputing and Networking Centre), Portugal (FCTUC - Faculdade Ciencias e Tecnologia da Universidade de Coimbra), Serbia (IPB - Institute of Physics, Belgrade), Spain (BSC – Barcelona Supercomputing Centre - Centro Nacional de Supercomputación), Sweden (SNIC – Swedish National Infrastructure for Computing), Switzerland (ETH Zurich - Swiss Federal Institute of Technology Zurich,

CSCS – Swiss National Supercomputing Centre), Turkey (UYBHM - National Centre for High Performance Computing (Ulusal Yuksek Basarimli Hesaplama Merkezi), UK (EPSRC – Engineering and Physical Sciences Research Council).

The principal **DEISA partners** are: RZG (Rechenzentrum Garching of the Max Planck Society, Germany), LRZ (Leibniz Computing Centre of the Bavarian Academy of Sciences and Humanities, Garching, Germany), BSC (Barcelona Supercomputing Centre (BSC) - Centro Nacional de Supercomputacion, Barcelona, Spain), CINECA (Consorzio Interuniversitario, Bologna, Italy), CSC (CSC- IT Centre for Science Ltd, Espoo, Finland), ECMWF (European Centre for Medium-Range Weather Forecasts, Reading, UK), FZJ (Forschungszentrum Jülich, Germany), IDRIS (Centre National de la Recherche Scientifique - Institut du Développement et des Ressources en Informatique Scientifique, Orsay, France), SARA (SARA Computing and Networking Services Amsterdam, The Netherlands), EPCC (The University of Edinburgh, Edinburgh Parallel Computing Centre, Edinburgh, UK) and HLRS (High Performance Computing Centre Stuttgart, Germany). The associate partners are: CEA Computing Complex (Bruyères-le-Châtel, France), Joint Supercomputer Centre of the Russian Academy of Sciences (Moscow, Russia), Swiss National Supercomputing Centre (Manno, Switzerland) and The Royal Institute of Technologies - Centre for Parallel Computers (Stockholm, Sweden).

17g) History and evolution

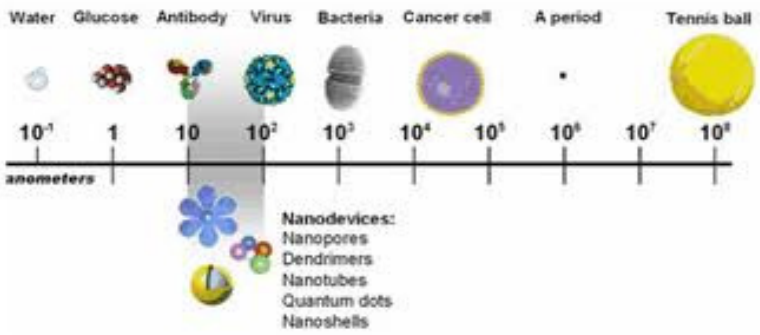
PRACE was the result of the awareness in 2005 that Europe was losing its grip on the frontiers of Computational Science. The High Performance Computing in Europe Taskforce (HET) established in 2006 by 11 countries developed a scientific case for high-end computing in Europe and provided recommendations for building a sustainable HPC ecosystem in Europe. PRACE was then valued by ESFRI as a RI. In April 2007 14 members signed the PRACE MoU. A proposal for a preparatory phase project (PRACE-PRO) was approved and the two-year project started in 2008. The first implementation phase project (PRACE-1IP) started in April 2010 and has a two year duration.

The first DEISA project started mid 2006 under FP6 and had a duration of four years. It developed and established the basis for the current DEISA infrastructure. It was followed up by the FP7 DEISA2 project.

17h) Security

17i) Operations

4. The MNT Collaboration Facilities Interchange RI Framework



4.1 MNT National Research Centres / Facilities

(C18) The Irish Tyndall National Research Centre

national access programme
.....National Facilities, National Access.....

Web Site / Document repository / Wiki: www.tyndall.ie/nap

Contractual documents:

Contact person: Julie Donnelly (julie.donnelly@tyndall.ie)

18a) Description of RI

The *National Access Programme* (NAP) offers researchers in Ireland access to the facilities and expertise available at the Tyndall National Institute (Tyndall). Tyndall is Ireland's largest research centre in *Information and Communications Technologies* (ICT) and has extensive fabrication facilities for both silicon and compound semiconductor devices as well as extensive facilities for photonics, nano/microelectronics and Microsystems research.

NAP enables all researchers based in Irish Universities and Institutes of Technology to engage in collaborative research projects which are undertaken at Tyndall. Projects range in scale from simple equipment access taking a number of weeks to broad projects requiring design, device fabrication, packaging and characterization that may be over twelve months in duration. NAP was established by *Science Foundation Ireland* (SFI) in 2005 and has recently secured further funding for five years.

18b) PA/NC collaboration explanation

The funding for NAP comes from a PA (SFI) and is distributed by an NC (Tyndall). SFI regularly reviews the activities of Tyndall in relation to how the funds are allocated.

18c) Budget, funding model, economic sustainability

To date SFI have funded NAP at an average of 1,5 M€ per year since 2005. The NAP model is based on the EU model for funding access to infrastructure - SFI provide an annual grant to Tyndall to administer on its behalf. Tyndall was previously part of the EU funded Programme RIMDAC (1999-2003) which funded trans-national access to Tyndall – NAP was established to replicate this model on a national-scale.

SFI award an annual budget to Tyndall and this covers the project fund (~0,85 M€), core staff (~0,35 M€), Capital Equipment (0,3 M€):

- the project fund is administered by Tyndall, but all the decision on what projects are funded is made by an independent Access Committee;
- 70% of the core staff budget pays for NAP engineering staff working on the projects. The NAP team work directly on NAP projects but over 100 Tyndall researchers and engineers have participated in NAP projects. Their contribution is costed as part of the individual NAP project;
- the capital equipment is proposed by the wider research community and the decision on what is purchased is made by the external Access Committee.

Budget 2011:

- Income: 1,35 M€ (from SFI),
- Expenditure: 1,35 M€ (0,7 M€ projects; 0,35 M€ core staff; 0,3 M€ Capital Equipment).

SFI will reduce the amount of the project fund awarded over the coming years to ensure the long-term sustainability of the Programme. Researchers will be encouraged to apply to other grant agencies (including the EU) to fund the work at Tyndall. SFI will continue to find the core staff and the capital Equipment elements of NAP for the next five years.

18d) Governance / Management

NAP is a Research Programme funded by SFI and managed by Tyndall. It is governed by an external Access Committee. This 17 member committee is made up of senior academic representatives of each of the nine Universities and the seven of the large Institutes of Technology with an independent chairperson. The Access Committee provides independent oversight of NAP, decides what projects are funded and also what Capital Equipment is funded.

Each year SFI holds an independent international review of the Programme. The purpose of the review is to evaluate NAP against international standards and recommend any changes or improvement to the Programme. NAP has always been rated very highly in these international reviews.

Within Tyndall, NAP is managed by a dedicated NAP manager who is responsible for the management of the Programme and the NAP team. The NAP Management Team,

representing senior Tyndall management, provides oversight of NAP. There is also a NAP Task Force made up of researchers and engineers that are actively involved in NAP projects and they provide feedback on the day-to-day workings of NAP.

18e) Users and interaction model

Since 2005, NAP has funded 249 projects for researchers in all nine Universities and the Institutes of Technology active in ICT research. The researchers are from all scientific disciplines and proposals have been received from over 60 different University Departments. While the majority of proposals come from Physics and Engineering, other areas have participated including Chemistry, Computer Science, Mechanical Engineering, Biotechnology, Microbiology, Pharmacy, Physiotherapy, Zoology, and Marine research. This diversity is a strength of the programme and involves a lot of discussion at enquiry/pre-proposal stage, in particular with researchers not familiar with device fabrication techniques, where Tyndall researchers work with the external researchers to define research projects and build on both sets of expertise.

User Access:[15] User access is made initially by users submitting an enquiry to NAP. The enquiry is evaluated by Tyndall experts and if the work can be done then the user submits a short proposal form to NAP. This proposal is costed and sent to the external Access Committee for evaluation. If the external Access Committee approves the proposal then the project can start as soon as possible. If clarifications are required then the users are asked to provide these clarifications before the proposal is approved. If the proposal is rejected then the user will be given feedback and may be given the option to re-apply. The time-line from proposal receipt to approval is usually an average of eight weeks. For smaller projects this may be as short as four weeks.

The NAP team at Tyndall actively promotes NAP through Workshops and Open Days and by regular visits to the research teams at their own Universities and Institutes of Technology. Users are given every assistance while writing their proposals to ensure that they maximize the use of the facilities to best support their research. Researchers from disciplines not familiar with ICT technologies are very much encouraged and guided through the process. Postgraduate students are also encouraged and travel and subsistence is covered by the grant to encourage a hands-on approach to the access where possible.

18f) Countries and international collaborations

NAP was established to fund national access to Tyndall in order to complement the European model of funding trans-national access. SFI extended NAP to Northern Ireland in 2007, but does not fund any other trans-national access. As the nature of the funding changes over the coming years it is likely that the NAP team will look for academic collaborators outside Ireland. It should be noted that research groups in Tyndall actively engage with other countries around the world through a wide range of funded programmes.

[15] Procedure from: www.tyndall.ie/nap.

18g) History and evolution

NAP has been a very successful Programme to date with a high emphasis on promoting collaboration and extensive outputs in terms of publications, generation of further funding and patents, licenses and a spin-out company. NAP is based on the European model of providing fully funded trans-national access to key research infrastructure. The current model of fully funded access works very well as it offers users a straight-forward route to access. The disadvantage of the model is that it relies on continuous funding from the funding agencies which raises a question about long-term sustainability.

In the last year the NAP team compared the current NAP model with models in other countries. The findings were that access models work best when user fees are kept low. Given the expense of doing customized research in large expensive infrastructure, this is difficult to achieve without additional funding from the agencies. Therefore support will continue to be required from funding agencies; either they provide the access grants themselves (as in the UK) or give the Institute the project fund to distribute on its behalf (as in the EU model and NAP). If the agencies are giving out the access grants they must be pro-active in ensuring that access to national infrastructure is encouraged and duplication of infrastructure is avoided. As NAP moves towards a new model where the users must apply to other agencies to pay for access it will be essential that the agencies actively support and promote these grant applications.

18h) Security

All users sign a NAP Memorandum of Understanding before a project starts and this outlines the protocols and rules governing NAP projects. Tyndall has well established policies regarding IP and Non-Disclosure and Confidentiality agreements. If users require additional specific agreements to be put in place, the drawing up of these is managed by the relevant offices at Tyndall. The vast majority of projects do not require additional agreements to be put in place. There is a very high publication output from NAP. Over 400 publications have resulted from NAP projects to date and NAP has contributed to 51 published theses to date.

18i) Operations

The services offered by NAP are fabrication facilities and expertise for silicon and compound semiconductor devices, for photonics, nano/microelectronics and Microsystems research. Facilities available include:

- Design, Modelling & Simulation Tools,
- Fabrication Laboratories,
- Microelectronics & Photonics Packaging Labs,
- Characterisation & Test Labs,
- Reliability Evaluation Labs.

(C19) The Belgian IMEC National Research Centre

Web Site : www.imec.be

Contractual documents:

Contact person: Cor Claeys (claeys@imec.be)

19a) Description of RI

IMEC is a world-leading independent research centre in nanoelectronics and nanotechnology. IMEC vzw is headquartered in Leuven, Belgium, has sister companies in the Netherlands (IMEC-NL) and in Taiwan, offices in the US and China, and representatives in Japan. Its staff of more than 1,750 people includes over 550 industrial residents and guest researchers. The multi-cultural research environment constitutes researchers and students from more than 60 different nationalities.

There are presently about 200 PhD students pursuing their research work at IMEC. IMEC's "More Moore" research targets semiconductor scaling for sub-22nm nodes. With its More than Moore research, IMEC invents technology for nomadic embedded systems, wireless autonomous transducer solutions, biomedical electronics, healthcare, automotive, photovoltaics, organic electronics and GaN power electronics. IMEC's research bridges the gap between fundamental research at universities and technological development in industry. IMEC's unique processing and system know-how, intellectual property portfolio, state-of-the-art infrastructure and its strong and worldwide network position IMEC as a key partner for shaping the future building blocks for a better life in a sustainable society.

19b) PA/NC collaboration explanation

IMEC vzw is a non-profit organization by Belgian law and headquartered in Kapeldreef 75 Leuven, Belgium. It has sister companies in The Netherlands (IMEC-NL, Eindhoven), Taiwan (IMEC-Taiwan, Hsinchu Science Park) and China (IMEC-China, Shanghai), and representation offices in the US and in Japan. IMEC vzw receives an annual grant from the Government of Flanders.

Fig. 11 – IMEC distribution of sites.

19c) Budget, funding model, economic sustainability

In 2010, IMEC revenue (P&L) was about 270 million euro. About 16% (44 M€) of the budget is an annual grant from the Government of Flanders, enabling the partial financing of IMEC's long term research which is crucial for the generation of critical strategic know-how. The other part of the budget is based on research financed by public co-funded programs (National research funds, European Commission, European Space Agency) and R&D performed with industrial partners from all over the world. IMEC has developed a dedicated business model for industrial collaboration (IMEC's Industrial affiliation Program) resulting in a strong leverage effect, cost sharing, risk lowering and shortening the development time. In selected technological fields the research is performed at IMEC by a consortium consisting of industrial (manufacturers, users, suppliers, software developers, etc) and academic (research institutions and universities) partners.

19d) Governance / Management

IMEC is a non-profit research centre with Headquarters in Leuven, Belgium. The governance is lead by the President and CEO and coordinated by the Executive Operational Board. IMEC also has a Board of Directors with representatives from industry, academia and government. Annually there is also a meeting of the internationally composed Scientific Advisory Board.

19e) Users and interaction model

The collaboration between IMEC and industrial partners can take different forms, e.g. (a) bilateral *agreements*; (b) *partnering* within the IMEC Industrial Affiliation Program; (c) technology transfer; (d) *licensing agreements* on process modules, complete process technologies or IP blocks; or (e) *training* activities.

The collaboration between IMEC and the scientific community can be performed under a variety of operation modes, depending on the final objectives. Typical examples are: (1) the *exchange of researchers* at different levels, i.e., graduate students, PhD students, post-docs or even senior researchers; (2) the execution of *dedicated processing activities*, jointly agreed between the requesting institute and IMEC; (3) *hosting research teams* to make use of the state-of-the-art facilities up to 300 mm wafer size; (4) performing *joint research activities*,

possibly within the framework of public financed projects; (5) *exchange of samples and/or data* resulting in jointly publications.

19f) Countries and international collaborations

IMEC is involved in a large number of projects within the EU FP7 program. Besides that, IMEC has R&D agreements with partners from all over the world. As an illustration the following geographical distribution of the bilateral contracts in 2009 can be mentioned: Belgium (25%), Europe (49%), Asia (7%), Japan (5%), US (12%), ROW (2%). In addition IMEC is collaboration with more than 300 different universities world wide. Another fully international IMEC program is the EUROPRACTISE service,

19g) History and evolution

In 1982 the Flemish Government set up a program in the field of microelectronics with the goal of strengthening the microelectronics industry in Flanders. The decision was inspired by the strategic importance of microelectronics for industry, and by the major investments required to keep up with developments in this field. IMEC was founded in 1984 by the Government of Flanders as a non-profit research centre and headed by Prof. R. Van Overstraeten. Over the last 25 years it has become a world-leading independent research centre in the field of micro- and nanoelectronics. IMEC's total staff has increased from 68 in 1984 to more than 1750 in 2010. Whilst about 70% of the total staff are on the IMEC payroll, the other co-workers operating at IMEC include industrial residents, PhD students, research fellows and exchange researchers coming from all over the world. IMEC's present position as a research centre is a direct result of the strong increase in international collaborations due to the presence of a state-of-art infrastructure and high-level advanced research carried out. Over the years IMEC has created more than thirty spin-off companies.

19h) Security

Over the years IMEC has achieved a well established *Security* and *Intellectual Property Rights* (IPR) control system, based on the strong experience of working with a wide variety of both industrial and academic partners. From a formal perspective, the IPR and confidentiality aspects for each interaction/collaboration/project are defined by standard legal agreements.

However, a case by case fine tuning and/or adaptation of these general rules is applied in certain specific projects.

4.2 MNT ROs Alliances and Collaborations for Transnational Access

(C20) The Epixnet Network of Excellence

Web site/Documentation repository/Wiki: www.epixfab.eu
Contractual documents: confidential
Contact person: info@epixfab.eu

20a) Description of RI

ePIXfab aims to offer prototyping access to silicon photonic IC technologies to fabless customers, and to promote take-up of silicon photonic IC technology. In this way, it plays a vital role in bringing silicon photonics from being a research item to the market. ePIXfab offers Multi Project Wafer prototyping and training, and (co-)organizes several outreach events per year.

20b) PA/NC collaboration explanation

ePIXfab is a collaboration between IMEC and CEA-LETI, with a collaboration agreement between the two institutes. ePIXfab is partially funded under the FP7 PhotonFAB project (Support Action).

20c) Budget, funding model, economic sustainability

ePIXfab is funded by the European Union, through PhotonFAB. No National Public Authorities were directly involved. Today, the funding still covers a large fraction of the operation. The funding covers the operational expenses for European users but not materials costs. The budget of ePIXfab covers around two FTE and expenses for travel, training and outreach events.
All process costs (substrates, mask, processing, dicing, ... cost of MPW dies or wafers) are fully paid by the user. The cost in a run is shared between the users, which makes the expensive technology affordable for universities and research institutes. The funding does (and did not) cover the operation for non-European users – these pay a margin on the price.

ePIXfab is collaborating with Europractice, the European Commission's cluster of ASIC services to increase pick-up of the technology and to ensure economic sustainability. PhotonFAB has brought the operation to a level of maturity where this is feasible. Since 2011, Europractice takes care of the MPW offer of sufficiently mature ePIXfab technology.

20d) Governance/Management

The collaboration is not a separate legal entity, but legally implemented as a collaboration agreement between IMEC and CEA-LETI. The longer-term management is the responsibility of a Steering Group with two representatives from IMEC and two from CEA-LETI, of which one is involved in silicon photonics and the other in the higher level management of the institute. IMEC currently coordinates ePIXfab; the daily management is performed by the ePIXfab coordinator at IMEC and the responsibility for ePIXfab at CEA-LETI.

20e) Users and interaction model

Users are research groups or researchers from world-wide universities, research institutes and companies. IMEC is the legal partner for the users, and takes care of the financial and legal implementation with the user. The collaboration agreement takes care of the legal and

financial implementation between the partners. Specific technical discussions are with IMEC or CEA-LETI directly. ePIXfab is for research only and based on the defined set of processes on offer only. Companies that need access to small series or low volume production, or research groups and companies that need access to tuned/optimized or other processes, work with IMEC or CEA-LETI directly.

Practically, the user signs the Terms of Use and can then submit designs to the MPW service. After wafer/sample delivery, IMEC sends the invoice to the user.

20f) Countries and international collaborations

The countries involved are currently Belgium and France. Increasingly, IMEC and LETI are collaborating with other European research institutes such as TNO, Tyndall, VTT and IHP. A support action proposal was submitted to FP7 widening the ePIXfab collaboration.
Users are world-wide, from Europe, North America, Asia, Middle East and Australia.

20g) History and evolution

The first silicon photonics multi project wafers were already executed within the FP5 PICCO research project, even for users outside of the project consortium. Getting sufficient use has therefore always been the core of the idea. This platform was more structurally set up within the FP6 ePIXnet Network of Excellence as a 'Facility Access Activity' by partner IMEC (year 1 and 2 of ePIXnet, 2004-2006). In year 3 and 4 of ePIXnet (2006-2008), the collaboration with LETI was founded and the MPW service continued within ePIXnet as the 'Silicon Photonics Platform'. Already then the mission was to increase take-up of silicon photonic IC technologies. The FP7 PhotonFAB support action was proposed in order to significantly reduce the still existing barriers for access (price, available technology, design ease, need for training, sustainability). PhotonFAB has set up a.o. access to more advanced technology, a design kit, training, a roadmap for access.

20h) Security

The Terms of Use signed by the user clearly state that all process IP and related information (design kit) is the property of the fab (IMEC/CEA-LETI), and that all design IP made by the user is the property of the user. (If the user includes third party IP in his design he is the sole responsible to have the necessary agreements in place.)

20i) Operations

ePIXfab operates MPW, training, outreach activities and the PhotonFAB project implementation with approximately two FTE.

(C21) The MNT Europe Project Collaboration

Web Site / Document repository / Wiki: www.mnteurope.org

Contractual documents: EU FP6 Contracts 506231 and 211564

Contact person: André Rouzaud, LETI, Arno Hoogerwerf, CSEM

21a) Description of RI

MNT Europe and its extension was an EU FP6 I3 project aimed at increasing the cooperation between five major European Research Institutes in the field of micro- and nanotechnologies: CEA-Leti, CSEM, FhG IISB and IZM, IMEC, and Tyndall Institute. The project consisted of Networking Activities and Joint Research Activities, but did not include Transnational Access, which later became a key element of the Framework 7 Programme.

21b) PA/NC collaboration explanation

The collaboration was between the five Research Institutes and funded by the EC as a project. No national Public Authorities were involved.

21c) Budget, funding model, economic sustainability

The budget of several millions of Euros for a three year period plus a one-year extension covered the *Networking Activities* (NAs) and the *Joint Research Activities* (JRAs) of the five RIs involved. A follow-up proposal was submitted to the EU, but was rejected. The partners still involved in the project keep in contact, even though this activity is no longer funded. Three partners of the project are now involved in the Heterogeneous Technology Alliance.

21d) Governance / Management

The project was managed by an *Executive Committee* with representatives of each partner (the two Fraunhofers counted as one partner). A *Governing Board,* with representatives of each partner, was in place to resolve any issues that could not be resolved by the Executive Committee. The Executive Committee operated as a very good team towards the end of the project.

21e) Users and interaction model

The project did not include a Transnational Access component, but the JRAs included teams of engineers from the different RIs. The goals of the JRAs were to develop demonstrators that involved the available technologies from at least two different RIs. Five different JRA projects were defined that resulted in demonstrators. The most important result however was that engineers from the RIs started to know their colleagues in other RIs. The Networking Activities foresaw the development of agreements on the subject of IP rights, marketing activities, and strategic coordination. An IP rights agreement was signed between the partners. It was agreed that for the sales of joint projects involving more than one RI, there would be a lead RI that would be responsible for all interactions with the customer. The contribution of the second RI would be arranged in a subcontracting agreement with the primary RI.

21f) Countries and international collaborations

The countries involved were Belgium, France, Germany, Ireland, and Switzerland. There was no other international cooperation.

21g) History and evolution

There was a long delay between the submission of the project proposal and the acceptance by the EC, so the project got off to a slow start. However, some of the first actions organized were mutual visits of the different RIs. This really contributed to a better contact between the partners. The members of the Executive Committee met at least twice a year in person and this helped to create excellent relations between the committee members. The JRAs were defined and started, which resulted in the creation of different engineering teams with contributions from different partners. The Networking Activities resulted in some serious thinking on how the cooperation between the different RIs could be achieved, given the fact that in some technical areas the different RIs are competitors, whereas in others, they are complementary. The two consecutive Project Officers were happy with the progress of the project and much effort was put into the proposal of the follow-up project, which envisioned an enlargement of the number of RIs involved and the addition of a Transnational Access component. The rejection of this proposal by the EC came as a total surprise and stopped an activity that was gaining momentum. Despite the lack of funding, the contacts between the members of the Executive Committee are maintained.

21h) Security

The model that has been developed of having one primary RI to interact with a customer and to use a subcontracting scheme for a second RI that has a complementary technology resolved many of the IP and confidentiality issues of the project.

21i) Operations

The follow-up of the project foresaw Transnational Access as a very important component and foresaw integration of complementary technologies at the assembly level. A major effort to define traceability of individual dies fabricated at different Research Institutes was also foreseen.

(C22) The Sinano Institute Collaboration

Web Site : www.sinano.eu

Contractual documents: Sinano Institute Statute (January 2008)

Contact person: Francis Balestra, Sinano Institute Director (balestra@minatec.grenoble-inp.fr)

Office: Grenoble INP-Minatec, 3 Parvis Louis Néel, 38016 Grenoble, France

22a) Description of RI

Founded in January 2008, the SiNANO Institute gathers twenty Academic Institutions (Universities and Research Centres) from eleven European countries. It is a non profit Association (French law), aimed at establishing a durable EU Network of researchers in order to form a *distributed Centre of Excellence in the nanoelectronic field*. It carries out a role of representation and coordination of the associated Organizations in the area of nanoelectronics. More than 900 scientific and technical staff work together in this field in the SINANO Institute. The SiNANO Institute office is located in Minatec.

SiNANO Institute's members are renowned European research organisations, universities and research centres in the field of nanoelectronics. Their competences are centred on the main Nanoelectronic domains, the "More Moore", "More than Moore" and "Beyond-CMOS" fields.

The Sinano Institute gathers *the most important flexible Research Infrastructures available in Europe for long term nanoelectronic research* (Joint Processing, Characterization and Modelling Platforms), particularly useful for downscaling in the nm range, use of non-standard processing and handling of new materials, direct contact with scientific staff and involvement of the requesting researchers in the infrastructure in collaboration with infrastructure supporting staff.

The networking actions in the Sinano Institute are intended to improve the individual and global competence by sharing experiences on basic problems (process step knowledge, …) and by covering a wide enough spectrum of device/system fabrication know-how to be able to receive and carry out external projects with the maximum of competence and efficiency: a project is handled by the facility that will have less need of new process development to do it and/or is able to do it within a minimum extension of time.

22b) PA/NC explanation

The Sinano Institute Research Infrastructure is a coordinated network of the *main national RI driven by the Academic communities* supported at different levels in the Member States.

22c) Budget, funding model, economic sustainability

Budget:

- initial investment: *290 M€,*
- annual investment: *19 M€,*
- annual running cost: *35 M€.*

Funding model:

- between 30% and 70% from National Funding,
- between 70% and 30% from European + National + Industrial Projects (*on average for the Sinano Institute Members: 50% National Funding / 50% Projects*).

22d) Governance / Management

- *legal entity*: French Association (Law 1901) of European Institutions;
- the *Statute* defines in particular the aim, the governance and the topics covered by the Association;
- *governance bodies*: General Assembly (including representatives of all the Members - annual meetings), Governing Board (five Members representing all the research areas – meetings every six months), Director of the Institute.

22e) Users and interaction model

Average number of external users per year (National, European, non-European):

- 1,200 external users coming from 25 (mainly European) countries (in average).

22f) Countries and international collaborations

The Sinano Institute gathers the following *20 Members*:

Grenoble INP (FR), Chalmers University (SE), IUNET (IT), KTH Royal Institute of Technology (SE), NCSR Demokritos (GR), Newcastle University (UK), Research Centre Jülich (DE), Tyndall Institute (IE), Université Catholique de Louvain (BE), Université de Lille (FR), University of Glasgow (UK), University of Liverpool (UK), University of Warwick (UK), University Rovira i Virgili / University of Granada (ES), Uppsala University (SE), Warsaw University of Technology (PL), Montpellier University (FR), University of Twente (NL), ICN (ES), ITE (PL).

The Sinano Institute is developing *European and International collaborations*. The Sinano Institute web site can also be used for requesting access to the Sinano Research Infrastructure (request form available).

22g) History and evolution

Research activities in the *FP6 SINANO Network of Excellence* (devoted to Si-based Nanodevices) emphasized the need to develop a network of flexible infrastructures for long term applications necessitating downscaling in the nm range, non-standard processing and handling of new materials. These long term activities are not realized on industrial platforms

which are often inappropriate, too slow, too costly or too risky for this long term research. Hence the Sinano Institute was created in 2008 for the *durable integration of the main European Academic Partners* working in the Nanoelectronic domain.
The joint management of this network of RI provides Europe with a unique tool for long term research and projects. These joint platforms are for instance presently used in the FP7 Nanosil (Silicon-based nanostructures and nanodevices for long-term nanoelectronics applications) and Nanofunction (Beyond CMOS Nanodevices for Adding Functionalities to CMOS) Networks of Excellence.

22h) Security

When the best Sinano Infrastructure(s) has(ve) been chosen, depending on the request and the competence of the Members, the access procedures are managed by each Sinano Member.

(C23) The MNT Heterogeneous Technology Alliance (HTA)

Web Site / Document repository / Wiki: www.4-labs.com

Contractual documents: *confidential*

Contact person: info@4-labs.com

23a) Description of RI

Four microsystems Research Infrastructures (CEA-Léti-Liten, Fraunhofer Gesellschaft Microelectronic Alliance, VTT, and CSEM) have signed an agreement to cooperate. A sales organization (4-Labs) has been founded to represent these RIs outside their home countries. Moreover, this sales organization also represents the RIs at large international organizations.

23b) PA/NC collaboration explanation

The cooperation is a purely private effort of the four participating RIs. No public authorities are or have been involved in this cooperation.

23c) Budget, funding model, economic sustainability

Initial funding for the activities of 4-Labs has been granted by the participating institutes. The goal is that 4-Labs becomes self-sufficient, with its income coming from commissions on the sales of projects. No European funding has been obtained thus far for this cooperation.

23d) Governance / Management

4-Labs is a limited company. Representatives of the participating RIs are represented in its board of directors.

23e) Users and interaction model

4-Labs is an intermediary and once a project has been signed, the customer deals directly with the RI which has been chosen.

23f) Countries and international collaborations

The countries involved are: France, Germany, Switzerland, and Finland.

23g) History and evolution

LETI and CSEM signed a cooperation agreement in 2001 and have cooperated since on multiple industrial and European projects. The Fraunhofer VµE joined in 2006 in this agreement and VTT joined in 2008. 4-Labs started its operation in Feb. 2009.

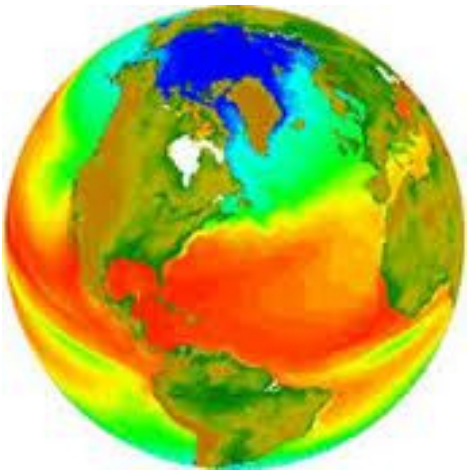
23h) Security

In general, each RI involved with a customer brings in its own technical know-how and IP. IP rights agreements are signed on a bilateral basis between the customer and a single RI for a particular technical subject.

23i) Operations

4-Labs employs 2.5 full-time employees.

5. The Research Data Infrastructure Framework



5.1 Digital Libraries and Infrastructures

(C24) The Open Access Infrastructure for Research in Europe

Web Site / Document repository / Wiki: www.openaire.eu

Contractual documents:

Contact person(s): Michael Hatzopoulos (Coordinator), Norbert Lossau (Scientific coordinator), Donatella Castelli (Technical coordinator)

24a) Description of RI

OpenAIRE aims to support the implementation of Open Access in Europe. It provides the means to promote and realize the widespread adoption of the *Open Access Policy*, as set out by the ERC Scientific Council Guidelines for Open Access and the Open Access pilot launched by the European Commission. OpenAIRE will establish the infrastructure for researchers to support them in complying with the EC OA pilot and the ERC Guidelines on Open Access. It will provide an extensive European Helpdesk System, based on a distributed network of national and regional liaison offices in 27 countries, to ensure localized help to researchers within their own context. It will build an OpenAIRE portal and e-Infrastructure for the repository networks and explore scientific data management services together with 5

disciplinary communities. It will also provide a repository facility for researchers who do not have access to an institutional or discipline-specific repository.

OpenAIRE's three main objectives are to:

i) build *support structures for researchers* in depositing FP7 research publications through the establishment of the European Helpdesk and the outreach to all European member states through the operation and collaboration of 27 National Open Access Liaison Offices;

ii) establish and operate *an electronic infrastructure for handling peer-reviewed articles as well as other important forms of publications* (pre-prints or conference publications). This is achieved through a portal that is the gateway to all user-level services offered by the e-Infrastructure established, including access (search and browse) to scientific publications and other value-added functionality (post authoring tools, monitoring tools through analysis of document and usage statistics);

iii) work with several subject communities to *explore the requirements, practices, incentives, workflows, data models, and technologies* to deposit, access, and otherwise manipulate research datasets of various forms in combination with research publications.

24b) PA/NC collaboration explanation

OpenAIRE is a FP7 CPCSA three-year project (n. RI-246686) started on 1/12/2009 involving 605 PMs with a total planned cost of five million Euros.

The *National Open Access Desks* connect researchers, research institutions, and policy makers at a national level on the one hand, and the OpenAIRE project services on the other. The OpenAIRE network of Open Access desks is structured similarly to the Europe-wide information network on European Research Programmes. The focus of the Open Access Desks activities is as support for compliance with the EC Open Access Pilot. The Open Access desks can be contacted for all questions on Open Access, depositing, the EC Pilot, etc. on the national level. Central support is provided through the OpenAIRE portal.

24c) Budget, funding model, economic sustainability

24d) Governance / Management

24e) Users and interaction model

24f) Countries and international collaborations

Each participating country is developing:

- a *National Research Environment* in terms of involved research institutions and national funding,
- specific *Open Access and Repositories* in terms of awareness, repositories, journals and organizations.

Each country has an active *Open Access Desk*.

The countries participating in the OpenAIRE infrastructure are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.[16]

24g) History and evolution

The development of Open Access and institutional repositories across Europe continues. The DRIVER project helped to establish and develop repositories in each of the European countries, and stimulated Open Access publishing by promoting policy development at the national level. COAR has been established to continue this work.

OpenAIRE builds on and provides access to the network of open access repositories already developed; and (in cooperation with other stakeholders, like COAR, SPARC Europe, and LIBER) it supports further expansion, so that authors have the possibility to comply with the EC Open Access Pilot and ERC Guidelines on Open Access within their own local context. OpenAIRE ties the publication to key research project data, so that it can be identified as an FP7 or ERC-funded project.

Summaries on Open Access and repositories in each of the countries participating in OpenAIRE are available on the *National Open Access Desk pages*. These also provide the contact details for the National Open Access Desks, who can provide support to researchers, institutions and repository managers in their own country seeking to comply with the EC Open Access Pilot and ERC Guidelines on Open Access.

24h) Security

Open Access is the immediate, online, free availability of research outputs without restrictions on use commonly imposed by publisher copyright agreements. Open Access includes the outputs that scholars normally give away free for publication; it includes peer-reviewed journal articles, conference papers and datasets of various kinds. Open Access provides the means to maximise visibility and availability, and thus the uptake and use of research outputs.

Access to knowledge, information, and data is essential in higher education and research; and more generally, for sustained progress in society. Access can be greatly improved. The digitising of research results and digital publication in recent decades represents a fundamental shift away from the “age of paper”. Improved access is the basis for the transfer of knowledge (teaching), knowledge generation (research), and knowledge valorisation (civil society). The central idea is that the results of publicly financed research should be available to the public.

It has been widely acknowledged that the journal subscription system that has been predominant in the last decades does not provide the wide, easy dissemination of research results that is wanted. It hampers the efficiency of the scientific research process, and the effective use and impact of public grant money. Even if a journal is available online, this does not mean it is freely available: university libraries pay large subscriptions to allow their

[16] More information is found in: www.openaire.eu/en/nlo/country-information.

academics to easily access journal materials online. Annual price increases that are many times the rate of inflation aggravate the situation. Matters are even worse in the developing world, where journal subscription prices mean that many institutions simply cannot afford access to up-to-date research. Some publishers do take special measures in such cases, but this is just dealing with the symptoms rather than with the cause of the problem.

Open Access addresses these problems *by taking the results of research that has already been paid for and making it freely available online*, through repositories, open access journals and websites. This process can provide significant advantages for individual authors, for researchers, for institutions and for the research process generally by freeing up the dissemination process. Many funders have recognised that the job of research is only half done if the results of that research cannot reach the widest audience – including small businesses, science journalists, practitioners and the general public wishing to stay informed. In Europe, it has led to the *EC Open Access Pilot* and *the ERC Guidelines on Open Access* supported by the OpenAIRE project.

Major advantages of open access are the *free availability of research results*, *high visibility* and *increased use and citation*. It also gives authors more control over their own publications.

There are also reservations about Open Access. It has been suggested for example, that *it interferes with peer-review*. This is not the case. *Open Access repositories supplement and do not replace journals*. The EC Open Access Pilot explicitly asks for the final, peer-reviewed and revised version of the article. Furthermore, some authors have feared that wider availability will increase plagiarism: in fact, if anything, Open Access serves to reduce plagiarism. When material is freely available the chance that plagiarism is recognised and exposed is much higher.

24i) Operations

(C25) The EUDAT (EUropean DATa) Project

Web Site / Document repository / Wiki: www.eudat.eu

Contractual documents: none

Contact person: Kimmo Koski

25a) Description of RI

EUDAT is a project aimed to create a collaborative scientific data infrastructure with the capacity and capability for meeting future researchers' needs in a flexible and sustainable way, across geographical and disciplinary boundaries. During its three-year funded life, the EUDAT initiative will undertake the first comprehensive European review of the approaches to deployment and use of a common and persistent data e-Infrastructure, the services being built and delivered on top of this infrastructure and the limitations of its services. EUDAT will deploy within its first phase a range of mature technologies (single sign on, data access and upload, long-term preservation, persistent identifier service, workspaces, web execution and workflow services, etc.) as shared services within a Collaborative Data Infrastructure for e-science and make those services available to researchers from a range of fields of science.

25b) PA/NC collaboration explanation

The EUDAT consortium brings together e-infrastructure providers, research infrastructure operators, specialist application/solution providers and researchers from a range of scientific disciplines under several of the main ESFRI themes. The depth and breadth of coverage allows a collaboration between for example, data centres such as JUELICH, KIT, CSC, BSC, SIGMA, SARA and SNIC, that support multiple customer groups as well as three infrastructure-providers (CSC, PSNC and SIGMA) operating 'end-to-end' across the networking, grid, HPC and data-management layers of the e-Infrastructure. Equally important, given the goal of self-sustaining operation within three years, is the involvement of two agencies with national funding responsibilities (SNIC, STFC) able to litmus test the proposition as it emerges.

25c) Budget, funding model, economic sustainability

EUDAT is a three year project which will mobilise some 2,469 person months, (68 full-time equivalent staff). The budget planned for the EUDAT first three-year phase is 30M€, with

55% coming from the European Commission, and 45% from the partners involved. There are also significant 'off-budget' items: personnel costs for two self-funding partners listed as beneficiaries, effort provided by other collaborators, and the cost of infrastructure provision (compute resources, storage, etc.).

Developing appropriate funding models to enable the infrastructure to be economically sustainable after the first phase is a specific task of one of EUDAT's work packages (WP2 "Sustainability and Evolution").

25d) Governance / Management

There are two main governing bodies in the EUDAT governance structure: the *General Council* (GC) and the *Executive Board* (EB).

- The purpose of the General Council is to protect the contractual interests of each partner (one member-one vote) and the project as a whole – that is, it controls distribution of grant, changes to the grant agreement and can change the coordinator. It delegates execution of the grant agreement to the Coordinator and the Executive Board.
- The EB is the executive decision-making body. The purpose of the Executive Board is to support the Coordinator, both in terms of the project Description of Work (which is part of the grant agreement) and supervision of the execution of work packages. The constitution of the EB provides voting rights for the Project coordinator, the scientific coordinator, the leader of WP2, responsible for long-term sustainability and four consortium members elected annually by the GC.

In addition to the governing bodies, there are three advisory bodies: the *Services and Architecture Forum* (SAF), the *Sustainability Committee*, and the *Advisory Committee*.

- The SAF provides an informal advisory platform in which technical discussion over service development and architecture takes place, and through which the participants in SAs and JRAs can explore issues to be taken to the EB by the scientific coordinator (who is also the head of the SAF).
- The consortium also plans to set up two external advisory bodies, one concerned with long-term sustainability, the other with the quality and value of the services being planned and offered. It is intended that the latter has an international character.

General management of the project is carried out by the Coordinator which provides a Project Manager responsible for the day-to-day management of the project, and an administrative project office, including financial and legal services. Work Packages are the bodies with delegated day to day responsibilities for execution of a group of related tasks and deliver agreed results to agreed standards. These operate in a transparent way, making up-to-date status information available to other parts of the project.

25e) Users and interaction model

In terms of the research communities, which contribute 40% of total project effort, the project has a diverse mix of interests and expertise from partners or associated members representing 15 specific research disciplines across all major fields of science (BMS, *Energy*, *Environmental Sciences*, *Material Science*, *Physical Sciences*, and SSH). These communities are represented in the EUDAT consortium by one or several partners and are actively involved in the building of the data infrastructure and its services. They also provide the contacts with the initial users of the infrastructure.

By the end of the third year, the EUDAT consortium expects to have forty communities with data stored within the EUDAT infrastructure, and 5,000 researchers actively using EUDAT services. The integration of the users beyond the initial communities involved in the consortium and the development of service delivery and usage models is a task of one of EUDAT's work package (WP2: "Sustainability and Evolution").

25f) Countries and international collaborations

The EUDAT consortium involves 13 European countries:

- Finland (CSC),
- Spain (BSC, RedIRIS),
- France (CERFACS, CINES, MaatG),
- Switzerland (CERN),
- Czech Republic (CUNI),
- Germany (JUELICH, DKRZ, EKUT, RZG, KIT),
- Austria (EAA),
- UK (EPCC, STFC, UCL),
- Italy (INGV, CINECA),
- Poland (PSNC),
- The Netherlands (SARA, MPI-PL),
- Sweden (SNIC),
- Norway (SIGMA).

EUDAT intends to pursue active collaboration with relevant data and e-Infrastructure initiatives in Europe. Collaboration with scientific communities beyond the initial communities present in the consortium will be sought in particular, as a way to expand the use of the EUDAT infrastructure. A framework for effective collaboration with other pan European e-Infrastructure activities (such as GÉANT, PRACE and EGI) and the ESFRI and SDI projects will also be designed. Collaboration agreements have also been defined with five large US based data initiatives which are willing to collaborate with EUDAT on a number of matters related to data management.

25g) History and evolution

The EUDAT project has its origins in the work of the PARADE (*PARtnership for Accessing Data in Europe*) initiative, documented in the PARADE White Paper[17] in October 2009.

25h) Security

Operational security and security policies are the responsibility of a stand-alone Operational Security Coordination Team which includes a *Computer Emergency Response Team* (CERT), responsible for security audits and operational security assessments.

Data authenticity, integrity and security tests will be conducted periodically in accordance with the quality plan.

Issues of trust are addressed at two levels: trust of the *data* through implementation of robust solutions to the integrity of preservation processes, privacy/security and data-provenance; and trust of the *service-provider* through transparency, involvement of user communities and long-term business plans.
The consortium agreement will define the terms of use of Foreground and the exclusion, if necessary, of Background IPR. It will also define each partner's obligation to protect Foreground and avoid infringement of third-party rights to Background IPR. Details of all Foreground IPR generated by the project will be recorded in an IPR Register. Shared ownership shall be avoided wherever possible, as will the use of open source software constrained by Controlled License Terms.

25i) Operations

EUDAT services and operations are defined in a specific work package (WP6: *Operating the European Collaborative Data Infrastructure*). This work package provides full-lifecycle data management services within a federated European Data Infrastructure, ensuring the authenticity, integrity, retention and preservation of data deposited by its users, especially those marked for long term archiving. The activities needed to ensure the deployment of services include the set up of a federated operation team on each site, the provision of a site registry with scheduled downtime monitoring, the actual provision of the core services (including deployment, operation and maintenance of the service), resource provisioning and registry, user-related services and internal support services, security and quality control, etc.

These activities represent around 20% of the total effort planned for the project.

5.2 Scientific Repositories collaborations

No cases were surveyed in this category.

[17] Editors: Kimmo Koski, CSC; Claudio Gheller, CINECA; Stefan Heinzel, RZG; Alison Kennedy, EPCC; Achim Streit, JUELICH and Peter Wittenburg, MPI-PL.

5.3 Arts and humanities, social sciences

(C26) The Digital Cultural Heritage Network (DC.NET)

Web Site: www.dc-net.eu

Contractual documents:

Contact person: Antonella Fresa

26a) Description of RI

DC-NET is *not* an e-Infrastructure or Research Infrastructure.

DC-NET is an ERA-NET project in the 7th framework programme of the EC. DC-NET is checking how existing e-Infrastructures can be used in the domain of digital cultural heritage and will define priorities in their research topics to take as much advantage as possible of the new perspectives that are created by using national and international e-Infrastructures. Finally the project will input its results to the *Joint Programming Initiative for Cultural Heritage* and will define the possibilities for a *Digital Cultural Heritage Data Infrastructure*.

26b) PA/NC collaboration explanation

N/A

26c) Budget, funding model, economic sustainability

DC-NET is mainly funded by the EC with a contribution by the project partners.

A follow-up project proposal has been submitted to realize the Cultural Heritage Data Infrastructure and this new project will define a *sustainable model* for that Data Infrastructure.

26d) Governance / Management

N/A

26e) Users and interaction model

N/A

26f) Countries and international collaborations

The project involves eight countries: Italy, France, Sweden, Estonia, Greece, Hungary, Slovenia and Belgium.

26g) History and evolution

N/A

26h) Security

N/A

26i) Operations

N/A

(C27) DARIAH ESFRI

Website: www.dariah.eu

Document repository / Wiki: internal only

Contractual documents:

Contact person: Laurent Romary

27a) Description of RI

The mission of DARIAH is to enhance and support digitally-enabled research across the humanities and arts. DARIAH aims to develop and maintain an infrastructure in support of ICT-based research practices and is working with communities of practice to: (a) *explore and apply* ICT-based methods and tools to enable new research questions to be asked and old questions to be posed in new ways; (b) *improve* research opportunities and outcomes through linking distributed digital source materials of many kinds; and (c) *exchange* knowledge, expertise, methodologies and practices across domains and disciplines.

27b) PA/NC collaboration explanation

The structure of DARIAH is based on the collaboration of different scientific communities in the Arts and Humanities of several European countries. See also the paragraph on *Security*.

27c) Budget, funding model, economic sustainability

The funding of the ESFRI project DARIAH has been covered by the European Commission during the Preparatory phase. For the upcoming Construction phase it has been calculated that an amount of about 4 Mio Euro per year, mainly covered by in-kind contributions, will be required. The percentage of fees each Member has to contribute to DARIAH has been calculated in accordance to the GDP of 2010. Thus far most part of the contributions is reserved for technical and scientific activities.

27d) Governance / Management

The DARIAH ERIC Consortium consists of the following bodies: *General Assembly*, *Board of Directors* (BoD), *Virtual Competency Centres* (VCC) with VCC Head, DARIAH-EU *Coordination Office* (DCO), and a *Scientific Advisory Board*. The *Executive Board* comprises the BoD, the VCC Heads, the Secretary General of the DCO, and one national representative of each Member or Observer partner.

27e) Users and interaction model

DARIAH will offer expertise and services to the scholarly community. The arts and humanities are very diverse and the DARIAH environment will therefore be structured into multiple segments and multiple entry points. In broad terms, DARIAH addresses distinct user communities (e.g. *philology*, *archaeology*, *European history*) in separate virtual research environment. These vertical pillars are horizontally based on (a) a technical infrastructure with APIs that can be addressed directly by software developers, as well as (b) clickable user interfaces for researchers.

27f) Countries and international collaborations

The following countries signed the Memorandum of Understanding on building the DARIAH *European Research Infrastructure Consortium* (DARIAH ERIC): Croatia, France, Germany, Greece, Ireland, Netherlands, Slovenia (all aiming at becoming Full Members), Switzerland, Italy (both aiming at participating as cooperating partners). The following countries are prepared for further collaboration with DARIAH: Austria, Denmark, and United Kingdom.

27g) History and evolution

As a project of the ESFRI Roadmap, DARIAH is required to pass through three phases. The DARIAH Preparatory Phase, intended to work out the concept of the DARIAH Research Infrastructure and the accompanying Business plan, ran from September 2008 until February 2011. The current transition phase concentrates on the set up of the Construction Phase. One project which will be built on the DARIAH infrastructure is the *European Holocaust Research Infrastructure* (EHRI)[18].

[18] See: www.ehri-project.eu.

27h) Security

DARIAH establishes a decentralized, federated architecture with multiple levels pertaining to security, including a decentralized authentication framework (in collaboration with other e-Infrastructure and ESFRI projects).

Rights management is particularly relevant in the context of restricted access to the working environment of research teams as well as licensed data sources (e.g. archaeology data with national laws constraining open access). In general, however, DARIAH promotes an open access / open data policy.

Apart from mechanisms for authentication, authorization and rights management, user trust is essentially tied to the longevity and authenticity of the data, e.g. through provenance mechanisms and persistent identification. These aspects of research infrastructures are key components of the DARIAH infrastructure.

27i) Operations

DARIAH is organised into four *Virtual Competency Centres* (VCC) which cover the following topics:

- VCC1 "e-Infrastructure" to establish a shared technology platform for the Arts and Humanities research,
- VCC2 "Research and Education" to expose and share researcher's knowledge, methodologies and expertise,
- VCC3 "Scholarly Content Management" to expose and share scholarly content, and
- VCC4 "Advocacy, Impact and Outreach" to interface to key influencers in and for the Arts and Humanities.

Other aspects regarding the financial model, the strategic direction, as well as the legal and governmental framework have been discussed during the Preparatory phase.

5.4 Health Sciences

No cases were surveyed in this category.

5.5 Natural Sciences and Engineering

(C28) Lifewatch – Italian National Network

Web Site / Document repository / Wiki:

Contractual documents:

Contact person: Saverio Vicario (Champion LW-ITA), Banki Olaf (coordination National Champions)

28a) Description of RI

Life Watch (LW) is a distributed RI that has as a goal to integrate data on environment and biodiversity from other RI (GBIF, National CHM, GEOSS, ..) and to offer a place to access an integrated virtual environment to share applications, workflow for integrated analysis powered by in-house computing farms and computing system put forward by other RIs (i.e. EGI, PRACE). Allowing scientists to work on shared virtual environment will not only increase collaboration and diffusion of best practices, but will also allow an easier transfer of knowledge from scientist to policy maker. Indeed policy makers would be allowed to access detailed results in a dedicated access to the same virtual environment. The RI is also interested in fostering more collaborations between scientists and citizens in view of a larger diffusion of the practice of the citizen scientist.

LifeWatch-Italy is the Italian network that will support the distributed RI by implementing the *Service Centre* (coordinating the access to the distributed service from the centralized portal) and the *Training Centre*. As specific national activities, LifeWatch-Italy will build a virtual institute for Biodiversity that will promote data production, analysis and interdisciplinary discussion on Biodiversity. The institute will start with four themes (Biomolecular Diversity, Collections, Species Interactions, Mediterranean Sea) that will unfold several e-services that will be accessible through LifeWatch RI and a few facilities that will help Italian scientists to increase high quality data production on Biodiversity.

28b) PA/NC collaboration explanation

LifeWatch will be an intergovernmental organization under the jurisdiction of the European Commission. Member of the organization include the state Public Administrations (PA) that are interested in the goal of LifeWatch. But, to work correctly LifeWatch will need to involve the scientific community. Within LW, the scientific community is represented by a National Champion that is a member of a National Network. Depending on the different countries, the option to participate in LW was promoted by PA or NC. The actual type of collaboration varied greatly among member states.

In Italy, participation was initiated by the scientific community with an informal committee of interested persons hosted by CNR-DSV director Giuseppe Martini. Italy participated as an observer in the planning phase of LifeWatch. Through a series of workshops promoted by CNR-DSV the committee enlarged and obtained legitimacy within the community. Only later did a PA become involved. The Italian National Network is working collegially and nominated a National Champion (Saverio Vicario) to interact with the European LifeWatch project.

The PA in LifeWatch is represented by MIUR (Ministry of Research and Education). MIUR has already signed a Memorandum of Intent and a *Memorandum of Understanding* (MoU) for the start up phase. The signature of the MOU for the construction phase will start the ERIC that will set up an official existence of the RI. The central position of the MIUR was defined in bilateral talks with MATTM (Ministry of Environment) and MPA (Ministry of Agriculture) that identified in the MIUR DG-I (DG of Internationalization of research) the reference PA for LifeWatch RI.

MIUR DG-I nominated as representative in the stakeholder committee of LifeWatch (the embryo of the general assembly – see governance section) a member of the Italian National Network (prof. Alberto Basset).

28c) Budget, funding model, economic sustainability

The budget for an RI that will service all EU member state was evaluated to be 250 million Euros for the first five years, both for construction and functioning. The actual budget for the five to eight funding countries is in preparation. Funding is supposed to come principally from member states. 85% as *in kind* framed with Service contracts between the national network and Central LifeWatch whilst 15% will come as direct cash contributions from representative member states (the MIUR in the case of Italy). The *in kind* contribution will be funded in part directly by the national government and in part by the research institutions that are part of the national network with dedicated personnel facilities). Private organizations could make deals with the central infrastructure or with the national network to support specific services. Users may pay some fee for access to dedicated computing power, although by statute (draft of the ERIC) this occurrence will need to be limited as much as possible.

Contribution of funding for the construction of the new service could come from grant money, FP7 has dedicated money for the ESFRI construction phase.

Five states, including Italy, initiated a start-up phase in January that should last one year and will lead to the signing of the final MOU. This phase has a budget of 500,000 euro per the three main member states and smaller contribution for the other two.

28d) Governance / Management

The draft of ERIC institutes a *General Assembly* with representatives from each member state PA. The General Assembly defines the policy and priorities and nominates a *Board* that has the goal to implement them and define a budget. The Board directly manages the 15% of in cash budget and indirectly manages the 85% via a defined service contract with the National Network. A small and independent scientific advisory board advises the general assembly on long term strategy while a *National Network Committee*, a *Data Provider Platform* (where representative from other RI or NOE provide data) and *User Forums* and *User Workshops* organized by the *Service Centre* inform, advise and interact both with the General Assembly and the Board on long term strategy and mode and quality of service implementation. Data production is not part of the goal of LifeWatch but a special provision was set up so that the general assembly could promote and financially support specific data production if that is recognized to be of global interest.

LifeWatch Italy, the Italian National Network, organized at the moment as a JRU headed jointly by the CNR *Department of Life Science* (DSV) and CNR *Department Land and Environment* (DTA), representing several Institutes (IBBE, ITB, IBP, ISMAR). The *Joint Research Unit* (JRU) also includes participation from several universities (Bari, Lecce, "TorVergata", Firenze), other research institution (*Stazione Zoologica di Napoli*, *Instituto Agronomico Mediterraneo di Bari*) and a private company (*Comunità Ambiente*). The JRU will be the basis on which the *Virtual Institute for Biodiversity* is funded.

28e) Users and interaction model

Three types of user are recognized: scientists, policy makers and citizens. All three will interact with the RI primarily through a central web portal. The central web portal will allow access to thematic virtual environments in which it will be possible to access raw and analyzed data, applications, workflows. All these services will be inserted in a social network framework making it possible to share, comment, score and tag data, applications and workflow. In particular, data comment and score will be a very useful method to tackle the complex problem, especially for biological data, of data curation (i.e. gene annotation, taxonomy update), showing what datum is controversial and requiring curation. The Service Centre will monitor jobs, queries and submissions and advise and put users who experience problems in contact with the service provider. Furthermore, the Service Centre and the Training centre will manage the User forum and organize periodic workshops to get feedback from users and train them in best practices towards utilizing the services.

LifeWatch will recognize three levels of access: world users, member state users, and paying users. Member state users will have access to specific subsets of data, while the paying user will be allowed to access dedicated computing resources.

28f) Countries and international collaborations

Italy, Spain, Netherlands, Hungary and Romania are part of the start up phase and signed a *Memorandum of Intent* (MoI) for the ERIC and a MoU for the start up phase. Sweden, Belgium, Austria, Finland, Norway have signed a MoI and already have a plan and funding mechanism to start the construction phase once the ERIC has been signed. Greece, Germany, Turkey, United Kingdom, and France are interested and participated as observers but are yet to sign the MOI. A FP7 project (CreativeB) is in approval phase and aims to coordinate the effort between LifeWatch and other International RIs. *Network of Excellence* (NoE) like MARBEF, MarineGenomics, Alternet (that is part of the international initiative LTER) sustain LifeWatch and contributed to the formation of the National Network in the different states.

28g) History and evolution

The problems of data sharing and integration and having a virtual environment for interdisciplinary collaboration are crucial for Biodiversity & Environmental studies. Land use management and fundamental understanding of Ecology and Evolution require the integration of disparate biotic (genetic, morphological, physiological, behavioural data) and abiotic (climate, physical and chemical attribute, geography/connectivity) types of data in a spatial and temporal context. But each of these types of data is collected with an approximation and standard that are specific to the community which make these observations. Furthermore, each type of data is collected independently by researchers given the distributed and variable nature of the biological phenomenon called Biodiversity.

The history that will follow is partial, and biased by the point of view of the writer, given that interest for biodiversity springs from different communities that have independently converged in RIs like LifeWatch. In particular this reconstruction lacks an ecological perspective of the problem.

Several initiatives started to promote data sharing standards and use of informatics within each community. The first to start was the genetic community with the rise of Bioinformatics and centralized DataBases (NCBI, EMBL, DDBJ). More recently the taxonomic community made a push towards the standard use of species names with projects such as Species2000 (later Catalogue of Life), PESI. Projects like EDIT or KeyToNature set up the technological and informatics tools for species description and diagnosis in a shared framework.

The need to connect the different approaches to study biodiversity in a more systematic and automated way forms the basis of several parallel initiatives. The Barcode Initiative developed in the CBOL and IBOL consortia makes a strong push for a systematic link between the genetic and organismal view of the species. MarineGenomics NOE was a big effort to cross genetic, biochemestry and biogeochemical views to study marine life.

Finally the need to integrate biological data spatially and temporally forms the basis for another set of initiatives:

- GBIF (*Global Biological Information Facility*) has the goal of federating all catalogues of biological collections and allow access based on taxon and geography;
- the Biocase project built software and a reference standard (ABCD) to dynamically share information on collection among arbitrary set of DBs;
- LTER and ALTERNET are networks of sites which monitor biotic and abiotic parameters for a long period (at least ten years).

Beside this large movement towards data sharing and standard definition, the need for deployment of online software has emerged as a particular need from within the genetic community. Online applications have the double advantage of allowing developers to be less concerned by portability issues and for users not to need to worry about installation, version updating and managing computing resources. This release from portability concerns allows more concern to be focussed on interface and documentation. Again NCBI and EMBL started the trend with the BLAST and EMBOSS websites. The high computational needs of Phylogenetics, Population Genetics, Genomics and Metagenomics resulted in a push for a specialized HPC portal such as the Scandinavian Bioportal, the Italian LIBI portal, the Spanish PHYLEMON or the American CAMERA. The need for computing power was identified and contact was made between LifeScience communities and the EGEE (later EGI) computing grid system within projects such as LIBI and the European project EMBRACE. Beyond genetics, the project AQUAMAPS showed that species ecological niche modelling would benefit from distributed computing resources such as EGI.

EMBRACE also experimented in another way with a distributed computing effort and exposed online services based on web-services. The results produced an annotated catalogue of web-services called Biocatalogue. The use of web-services allows users to interact with flexible workflow engines such as TAVERNA and with dedicated social network style repositories of workflow such as MyExperiments.

In conclusion it should be added that for all this experience in biodiversity and environmental studies to be really spatially explicit it has to interact and be compliant with the Open Geospatial Consortium and the European directive Inspire.

GBIF at first had the vocation as Global Facilities to federate all the biological aspects of Biodiversity, but it became clear that only by including all the abiotic components would it be

possible to produce a useful output. For this reason LifeWatch RI came up with the goal to create a common working environment for biodiversity and environmental data. In this sense, Alternet, which includes sites with both biotic and abiotic measurements, was conducive for the LifeWatch creation.

28h) Security

The statutes push towards the use of open source software but allow for collaboration with private informatics firms.

LifeWatch will not be the direct curator of data that is actually stored by the national network or third parties. Once the data is shared in the system it will accessible to all users, except for a special provision in favour of user member states for some data.

Although a query system will access the different data sources in a transparent manner for the user, traceability will allow the user to obtain details on the source and filter based on trust of the different sources. User data comments, scoring and tagging will be additional criteria for filtering data.

The traceability is also relevant in allowing proper citation of previous work and to allow sources to monitor the impact of their work. For example, within taxonomy it has been proposed several times to use access to taxonomic reference collection as a measure of the quality and usefulness of the work of the professional taxonomist who produced the reference collection. This should provide an incentive for scientists and institutions to share their information.

The are as yet no exact definitions of protocols and procedures for the LifeWatch informatics system given that the LifeWatch project has not yet committed to a specific technology. The details will be defined between the Spanish National Network which has the duty to implement the IT LifeWatch core and the FP7 project ENVRI. The ENVRI project has the goal of defining the common IT solution for the environmental ESFRI, including LW.

28i) Operations

Italy, Spain and Netherlands decided that during the start up phase a virtual working environment for estuarine environment would be built and that the emphasis would be on studying invasive species as target parameters.

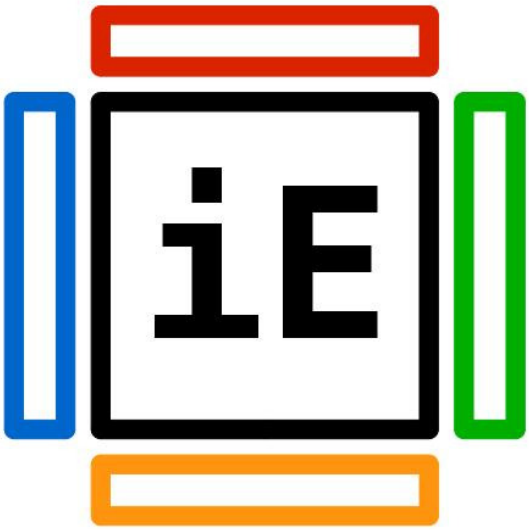
For this goal the Italian network wants to collect from all JRU members, species list and compare these with the official Italian check list of native species. Different national activities that involve biodiversity data integration are ongoing and involve members of the JRU and so could be the means to get starting data for a showcase of what could be Lifewatch in Italy.

The Italian network also wants to build the genetic tools (*sensu* Barcode) to identify invasive species even when not in an identifiable life stage (i.e. sample of plankton).

6. The Remote Instruments access model

6.1 The Instrument Element infrastructure model

(C29) The Instrument Element (IE) Infrastructure Access Model



Web Site / Document repository / Wiki: www.dorii.eu/resources:adaptation:middleware:IE

Contractual documents:

Contact person:

29a) Description of RI

Traditional Grids are composed mainly of computing and storage resources. The Instrument Element (IE) component, as its name suggests, adds the possibility of including such devices as scientific instruments and sensors in the data elaboration process. In other words, the Instrument Element represents a virtualization of data sources in a Grid environment.

The main goal of the IE middleware is to provide users with a simple way of attaching their scientific instrumentation to gLite-based grids. The IE framework provides support for secure access control, concurrency control, simple Grid storage access and JMS publishing. It offers a common interface for accessing instrumentation. Instruments and sensors are interfaced via Instrument Managers that allow connections to physical devices or more precisely, their control systems. Instrument Managers consist mainly of the Java client code for the instrumentation and should run inside the IE installation.
The IE has been adopted for attaching scientific instrumentation to the computing and storage Grids in a number of EC funded projects as well as in some regional projects. Also, it is internally used in Elettra.

29b) PA/NC collaboration explanation

29c) Budget, funding model, economic sustainability

29d) Governance / Management

29e) Users and interaction model

b, c, d, e:

The IE middleware has been developed with the support of EC projects and ELETTRA (see point g for details). The future of the IE middleware depends largely on support from the NGI (National Grid Initiative). The actual infrastructure management depends entirely on the owner / provider of the scientific instrumentation. The IE allows for simple integration of instruments into the Grid environment. The management policies, conditions, access rights etc. are determined by the instrument owner.

As an example, one may consider the use of the IE in the ELETTRA laboratory. The IE is used by beamline scientists on a number of beamlines to provide access to their instruments, store data and run on-line and off-line processing workflows on the Grid. In such cases, beamline users access the IE, and the instruments it controls, by authenticating themselves with user certificates (x509). The same certificates are used for authenticating users on the Grid. This model has been adopted by a number of applications of the DORII project, in particular by the oceanographic community.[19] It is also used by almost all ELETTRA users (1,000 a year) in a completely transparent way to access certain functions, such as account management from the centralized web portal. The IE has also been used to implement demonstrators for the NFFA EC project[20] and in a regional project for environmental monitoring using the Grid.

29f) Countries and international collaborations

The GRIDDCC project involved partners from Italy, Greece, UK and Israel.

The DORII project involved partners from Italy, Poland, Germany, Spain and Greece.

The ELETTRA is a multidisciplinary Synchrotron Light Laboratory in Trieste, Italy open to researchers in diverse basic and applied fields. The laboratory is equipped with ultra-bright light sources in the spectral range from UV to X-rays and offers a stimulating and competitive environment to researchers from all over the world.

29g) History and evolution

The *Instrument Element* (IE) concept was originally introduced by the GRIDCC (Grid-enabled *Remote Instrumentation with Distributed Control and Computation* – FP6 Specific Targeted Research Projects).

[19] See www.dorii.eu for more information.
[20] See: www.nffa.eu.

Following the completion of the GRIDCC project, the IE has been reimplemented from scratch at the ELETTRA Sincrotrone, Trieste in order to improve its functionality. The code has been actively maintained and further developed by the ELETTRA Scientific Computing Group with support from the DORII project.[21] DORII ended on July 31st 2010 and its continuation proposal has not been funded.

Since 2008, the IE has been endorsed by the EGEE's RESPECT programme and is included among the EGI's tools.

29h) Security

The Instrument Element runs as an Axis web service inside a Tomcat servlet container. The IE presents a SOAP web service interface for client access. The interface contains methods for controlling the Instrument Managers and thus the devices behind them, as well as the authentication methods. The framework does not provide a client GUI.

User authentication on the IE is performed using the gLite/GSI security model based on user's proxy delegation, with a fine-grain authorization control through *Virtual Organization Membership Service* (VOMS) attributes. The VOMS roles are mapped to predefined Instrument Element roles and may be modified by the administrator during runtime. Multiple virtual organizations are supported. The framework provides a Grid-FTP based utility that allows Instrument Managers to save their outputs to Grid storage elements or load data and settings from there. Middleware hides the complexity of the Grid protocols from the developer of the instrument interface. Users are authenticated on the Grid by their delegated proxies.
IE assures multiple user support through concurrency control and locking. Instruments can be explicitly locked by a single user for a certain time period, e.g. to perform a set of operations on the device. Locking and unlocking of the instrument manager is triggered by user-issued commands. Instruments are locked automatically by the framework during the execution of commands that change the state of the instrument or its parameters and attributes.

Instrument Element code is written in the Java programming language and is released as open source software under the DORII license.

29i) Operations

IE framework is installed and configured via an Apache Ant build file following the procedure described in the accompanying documentation. It requires a Linux system (preferably RHEL based) with Java SDK and a Tomcat server. The host machine must have a valid certificate. With security disabled, the IE may be installed on MacOS and Windows machines as well, but its functionality is crippled.

Instrument Manager (IM) is the code that connects the Instrument Element to the instrument's control system or, when possible, to the instrument itself. Instrument Managers are not standalone clients, once created they must be deployed to an Instrument Element installation and run inside it. Instrument Managers may be viewed simply as the Java client code for a specific instrument. Complexity of the Instrument Manager depends upon the

[21] *Deployment of Remote Instrumentation Infrastructure* – EC FP7/2007-2013, grant agreement RI-213110. See again www.dorii.eu for more information.

instrument's interface. In the best possible case, there is already a Java client available for the given instrument, so the Instrument Manager is simply a wrapper around it. The fastest and simplest way to build an Instrument Manager is to use the provided template and the Eclipse IDE. The template is intended as a guide and a starting point for development of the custom Instrument Managers. Both the template and especially the example code contain detailed comments for better understanding of the IM parts.

Users who desire to integrate their instrumentation into the Infrastructure using the Instrument Element middleware should install and configure the IE and develop an Instrument Manager for each instrument.

6.2 The Global Monitoring access model

(C30) The Global Monitoring Access Model (Cyclops)

Web Site / Document repository / Wiki: https://pop.cp.di.uminho.pt/cyclops

Contractual documents: DoW

Contact person:

30a) Description of RI

Civil Protection is a complex, multidisciplinary activity which involves high human and material costs. A large degree of heterogeneity of data sources, activities and expertise at regional and/or local CP agent level, can be seen in most EU countries. The problem is aggravated by the fact that this kind of activity frequently transposes country borders, notwithstanding some international projects intended to normalize data and procedures, mainly on geospatial or risk data acquisition. Another serious problem is the *insufficient level of collaboration between CP and R&D community*.

The EU Commission has stimulated cooperation between different EU countries, and even with other countries (EUA, Japan, India, Latin America, etc.), in the field of CP in order to decrease the high costs and also to increase the effectiveness of intervention on any type of hazards occurrence. The participation of the R&D community has been related largely to the simulation of natural or human-made disasters, as this kind of work is important in order to promote new procedures and even new equipment for hazard intervention. With increasing computational power and data acquisition capabilities, using new kinds of in-situ sensors and satellite features with just-in-time data availability, the R&D community can have real time or near real time intervention in CP procedures.

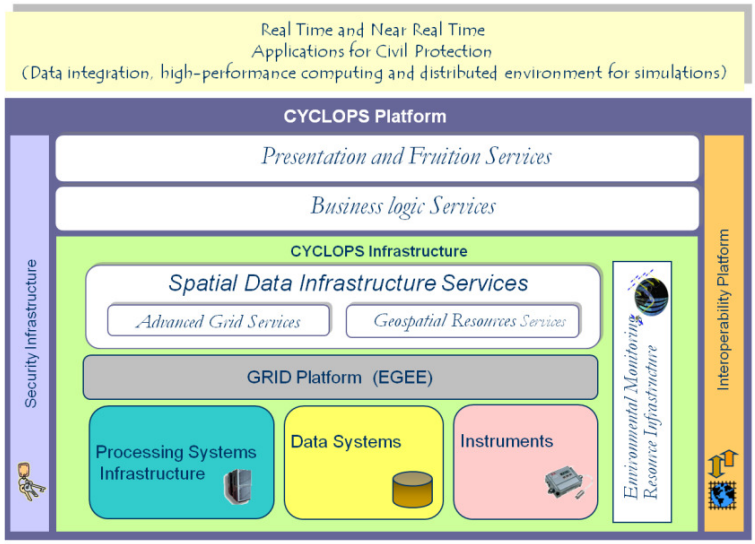


Fig. 12 – Overall architecture for an European e-Infrastructure for CP applications (image from Cyclops D16, page 18).

CYber-Infrastructure for CiviL protection Operative ProcedureS (Cyclops) is one of the first projects in Europe to include both R&D (mainly GRID researchers) and the CP community in order to develop a proof of concept in using a computational grid infra-structure to build real time or near real time CP applications.

The *Global Monitoring for Environment and Security* (GMES) concept was endorsed by the EU Commission in 2001, with the aim of "establishing by 2008 a European capacity for Global Monitoring of Environment and Security" to gather and use all available data and information in support of sustainable development policies. GMES has the potential to stimulate economic growth by creating innovative value-added services. The challenge for GMES is to use these services to enable decision makers to better anticipate or mitigate crisis situations and management issues related to the environment and security.

The Final Report for the GMES Initial Period recognised the European Civil Protection (CP) as one of the GMES service categories. This report outlines the importance of developing enabling e-infrastructures and virtual organisation services to serve specific GMES applications. Indeed, the EU EGEE (Enabling Grids for E-Science in Europe) project provides a powerful GRID platform to implement services for specific application Communities. However, GRID evolution has mainly focused on technology, whilst GMES services have mostly been user-oriented. Thus, there is a need to cross-disseminate the approaches, requirements and visions of the diverse Communities in order to fully exploit the GRID capabilities for GMES applications. CYCLOPS brings together these two important Communities: GMES and GRID, focusing on the operative sector and needs of European CP.

30b) PA/NC collaboration explanation

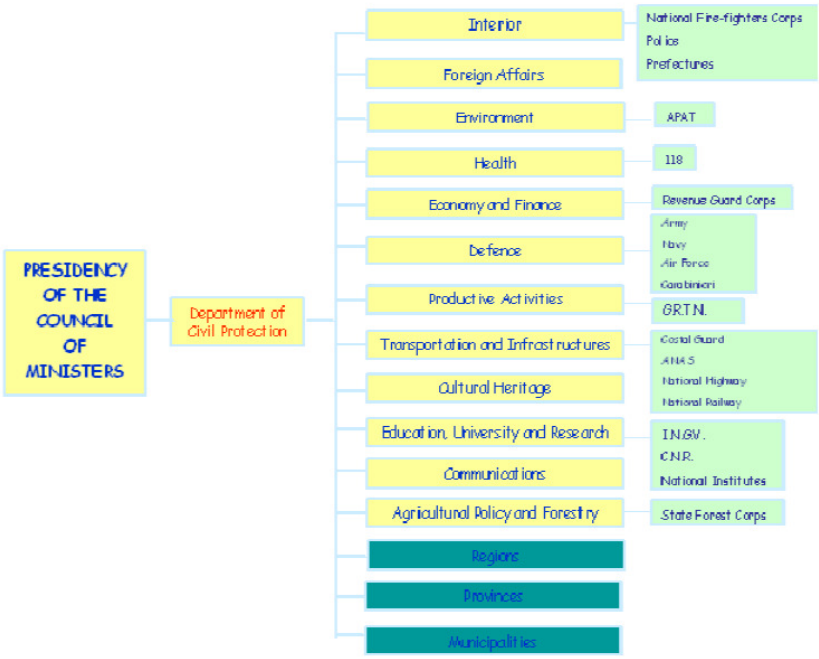


Fig. 13 – Example of PA/NC collaboration for Civil Protection: the case of Italy (from: Cyclops D6).

30c) Budget, funding model, economic sustainability

The Cyclops project has not reported any financial/economical evaluations for the funding and costs of the GMES infrastructure. It is clear however that such an infrastructure should have both National (from Civil Protection) and European funding. Grid or other ICT infrastructures used could charge for use according a specific agreed model (via resource sharing, as is for the grid, or via other business models found for instance in network or HPC).

30d) Governance / Management

The Cyclops project has not reported any suggestion for the governance of the GMES infrastructure. However one can suppose that for a stable GMES infrastructure, governance based on a distributed model, with some European coordination, is required.

30e) Users and interaction model

The users of the GMES infrastructure are specific Competence Centres of each National Civil Protection. For a detail of such structures, see Cyclops D6.

30f) Countries and international collaborations

(*from CYCLOPS D6, pag.148*) To date, *a real European cooperation in security civil domain between members of the European Union doesn't exist*. This collaboration between members

will become more realistic in the next few years. From an operational point of view, in the fire fighting domain for example, some non-official partnerships do exist between several countries. South European countries cooperate for external assistance in case of cross-border fires or insufficient national capacity to share competences and equipment. For this, the European Commission has set up *Monitoring Information Centres* (MIC) accessible and ready to intervene 24h/24, and the Common Emergency Communication and Information System (CECIS). Finally, the EU supports simulation programs for catastrophes, organized to evaluate the operational assistance and command chain and to test in full-scale the co-operative work between European teams. As for country coverage, it exists on an old *cross-border cooperation* (1963) between Italy and France.

For data and knowledge broadcasting, new programs have been developed in the last few years in a European context. The European initiatives GMES, or the INSPIRE program[22] could be quoted which aim at sharing spatial data between members.

The following are also relevant:

- PREVIEW: www.preview-risk.com,
- RISK-AWARE : www.smr.arpa.emr.it/riskaware,
- RISK-EOS: www.risk-eos.com/actus/pge/index.php?arbo=0,
- EUFIRELAB: www.eufirelab.org.

The establishment of a European Grid Platform must take in account all existing co-operations in the field of data sharing, data mining and skills exchanges.

European Forest Fire Information System

The European Commission DG Joint Research Centre, in 1999, set up a research group to work specifically on the development and implementation of advanced methods for the evaluation of forest fire risk and mapping of burnt areas at the European scale. These activities led to the development of the *European Forest Fire Information System* (EFFIS). Since 2003 EFFIS has been part of the Regulation (EC) No 2152/2003 (Forest Focus) of the European Council and Parliament on monitoring of forests and environmental interactions. All EFFIS activities are coordinated with the DG Environment to reach final users, Civil Protection and Forest Services in Member States. EFFIS is aimed at providing relevant information for the protection of forests against fire in Europe, addressing both pre-fire and post-fire conditions.

On the *pre-fire phase*, EFFIS is focused both on the development of systems to provide forest fire risk forecast based on existing fire risk indices, and on the development of new integrated forest fire risk indicators. These indices permit the harmonized assessment of forest fire risks at the European scale. They may be used as tools for the assessment of risk situations in cases in which international cooperation in the field of civil protection is needed. Currently, the dynamic forest fire risk forecast indices are available on the EFFIS web site and sent to the Member States Services daily from the 1st of May until the 31st of October.

On the *post-fire phase*, EFFIS is focused on the estimation of annual damage caused by forest fires in the southern EU. All burned areas larger than 50 ha, which account for around 75 %

[22] See: inspire.jrc.it

of the total area burnt in southern Europe are mapped every year using satellite imagery.The first cartography of forest fire damage in southern EU was produced in 2000 and continued for subsequent years. Additionally, as from 2003 a new activity for rapid assessment of forest fire damage has been developed in order to map all fires larger than 100 ha twice during the fire season: at the beginning of August and at the beginning of October.

An EU Fire Database is also included in EFFIS (previously referred to as the Common Core database). The database contains forest fire information compiled by some EU Member States.

The outcome of research topics on forest fires currently investigated at the JRC will be implemented in EFFIS in forthcoming years. These topics are all related to the post-fire phase and refer to forest fire atmospheric emissions, vegetation regeneration, and post-fire risk analysis.[23]

MeteoAlarm information system

Our climate is changing and extreme weather is likely to occur more frequently, increasing danger to life and damage to property. Time after time storms, floods, or avalanches somewhere in Europe have lead to disasters and heat waves over recent years and have cost many thousands of lives. Meteoalarm.eu provides *a single source of comprehensive weather conditions anywhere in Europe*.

Meteoalarm is a new website, designed to warn the public of severe weather across Europe. More than twenty European countries have combined to develop[24] a unique initiative from Eumetnet, the public European weather services network within the World Meteorological Organization. A universally understood system using symbols and colour-coded maps provides the latest warnings of expected severe weather for the next 48 hours over most of Europe. Wherever one is in Europe, clear, concise information will help one to plan travel, or any other activity which might be affected by severe weather.

Where, for example, might heavy rain cause flooding; what is the risk of avalanche; might fog delay my flight; and will hot, dry weather increase the risk of forest fires? Each country is colour-coded on the map to represent four levels of warning: red to indicate exceptional risk from dangerous weather conditions, down through orange and yellow to green, indicating that severe weather is not expected. The site also offers a greyscale map for colour blind people.

The alert levels are published in a unified system with a clear relationship between the meteorological feature towards possible damage and proposed functioning, this to avoid damages. The thresholds for these levels differ from region to region, because for instance intense snowfall in the Alpine region causes less disruption and damage than in Lisbon. Meteoalarm is also a portal to the national warning systems: click on the logo of individual weather services to visit websites of the respective national meteorological services for regional information.

The service focuses on Europe, but is meant for everyone in the world and is available in 17 languages. Not only do business and holiday travellers benefit, but so too will official

[23] See: effis.jrc.it/wmi/viewer.html.
[24] See: www.meteoalarm.eu.

organizations such as marine and mountain rescue services. People can use it to plan more effectively, businesses can prepare for how severe weather could affect their operations and emergency services will have up-to-date information close at hand. TV weather presenters in Europe may use the coloured map to enhance extreme weather.

30g) History and evolution

30h) Security

(*from CYCLOPS D16, Pag.43*) In the context of CP applications, security is one of the main issues. Security covers a wide range of aspects, from data access, to system availability and so on. To define security requirements and prepare a security plan and infrastructure, one generally accepted approach includes the following steps [RFC 2196]:

1. identify *what* you are trying to protect,
2. determine what you are trying to protect it *from*,
3. determine *how likely* the threats are,
4. *implement measures* which will protect your assets in a cost-effective manner,
5. *review the process continuously* and make improvements each time a weakness is found.

As a study for the definition of research strategies, the [Cyclops] documents focus on points 1 and 2 to identify which specific challenges CP applications pose in the design of an advanced e-Infrastructure.

A preliminary consideration is required concerning the point 2 [*perimeter*].

It is possible to broadly classify threats into two categories: threats due to *natural events* (like floods, fires, earthquakes, etc.), and threats due to *human actions* (errors and attacks). This classification is useful to highlight a point that distinguishes an infrastructure for CP application from many others. In fact for many applications, e.g. e-Business, e-Commerce or e-Government, human threats are the most important ones, because they are considered more probable. Therefore the corresponding infrastructures are designed to be protected mainly from these kinds of threats. On the contrary for CP applications, natural threats must be considered much more probable since they are the reason the infrastructure is developed. Therefore the infrastructure must consider what could happen to the resources located near the risk area under an emergency situation.

The example of SPC-GD, for flood management is symptomatic of the vulnerability of these real-time and simulated data. More widely, events such as Gard 2002 which resulted in important communications disconnections and crucial data exchange difficulties among all involved actors, illustrated the important need to secure essential data in remote sites outside the hazard locations.

This availability problem impacts on the general architecture of the system since it involves the basic communication infrastructures deployment, and should therefore be the subject of a specific study. For example, some grid utilities could be implemented to ease replica management and automatic job submissions in order to enable the expertise of other safe forecasting units – such as the *French National Hydrometeorological and Flood Forecasting Centre* (SCHAPI), which can provide its own expertise across all of French territory.

With regards to point 1 [*challenges*], in principle all the resources shared through the infrastructure at different levels need to be protected: computing and storage resources, communication lines, network systems, data, sensors, processing services, etc. However this document focuses in particular on data and services that, in the context of CP applications, are often characterized by complex data policies.

In the context of CP applications, types of exchanged data and their providers are characterized by great heterogeneity. The Final Report of "Data Policy Assessment for GMES" considered six common policy characteristics:

1) *ownership, privacy and confidentiality*: which concerns who owns data and who can access them;
2) *intellectual property rights and associated legal frameworks*: which concerns the assignment of property rights through patents, copyrights and trademarks;
3) *standards and metadata*: which concerns the adoption of common specifications for data formats, data quality and metadata;
4) *licensing, distribution and dissemination*: which concerns how data can be provided;
5) *pricing policy*: which concerns payments due for accessing and using data;
6) *archiving policy*: which concerns data preservation.

These are considered with respect to the main data providers for CP and GMES applications: statistical institutes, mapping agencies, institutes for natural resources, environmental monitoring and Earth Observation.

Based on the previous analysis, and taking into account the existence of different users/providers with different policies, the CYCLOPS Architectural Framework describes a distributed system characterized by sub-domains controlled by different organizations acting as users and/or providers. The existence of different data policies makes the boundaries between sub-domains significant. In fact each organization typically has its own security architecture made up of services, rules, people, processes and procedures. Therefore these boundaries are both logical (where ownership and related data policies change) and technological (because data policies are enforced through different technological solutions).

Actually the choice of a *Service-Oriented-Architecture* (SOA) for the CYCLOPS Platform was made taking into account these characteristics. Indeed SOA reflects the reality that ownership boundaries are a motivating consideration in the architecture and design of systems.

To make the CYCLOPS Architectural Framework feasible, the integration of the existing security infrastructures is required. Since the adoption of a new security infrastructure for all users is unfeasible, a federated approach is adopted. A *Federated System* (FS) is a collection of independent and autonomous systems which allow sharing of data and services. In federated systems a cooperative approach is adopted: participants agree on a set of common specifications to be used for sharing data and services. Common specifications concerning data formats, metadata, interfaces and protocols are required only to participate in the federation. Out of the federation scope, each participant can maintain its own infrastructure. This loose approach preserves participants' investments and facilitates sharing because participants do not need to change their infrastructure, they only need to extend it for enabling federation services and common specifications adoption. In the security context, the federation can be established providing common specifications for: (a) data (and services)

policy description and exchange, and (b) security services to support data (and services) policies.

The CYCLOPS Platform is [*was*] based on the EGEE infrastructure which provides a complete set of security services built around the concept of *Virtual Organization*. This means that all the resources shared through the Grid can be considered part of the same security sub-domain. Therefore another aspect that the security architecture of the CYCLOPS Platform should consider is the relationship between the CYCLOPS security services and the corresponding services provided by the underlying Grid.

30i) Operations

(*from CYCLOPS D6 Pag. 152-161*) Although there is much diversity and complexity in civil protection activities and organizations around the Europe, some common elements can be detected (Quarantelli, 2000). These common functions are very general and simple, however they allow one to understand and detect parts of operations of the Civil Protection agencies which could be commonly enhanced by Grid technology adoption.

- There are *shared responsibilities* among *three nested and prioritized levels* depending on disaster intensity. To control rescue phases, each level has an attached operational centre. For a *local* event, rescue monitoring is controlled by a local operational centre. *Regional* and *national* centres are only informed of the state of rescues. For an important crisis, control of rescues is taken in hand by higher levels services.
- From a local to a national implication in the rescue phases, many interactions and cooperation among the three levels (local, regional and national) are found. However, there is often poor integration between the higher and lower levels (Quarantelli, 2000).
- In the case of a major disaster, direction of the rescue is assumed by the Minister of interior. Depending on the type of disaster (natural, industrial, terrorist attack...), other ministers collaborate in decision making.
- The functioning of CP agencies is characterized by a dynamic structure adapted to the disaster conditions in near or real-time.

Finally, in terms of administrative organisation, these four countries have the same structures where there is a major government responsibility.

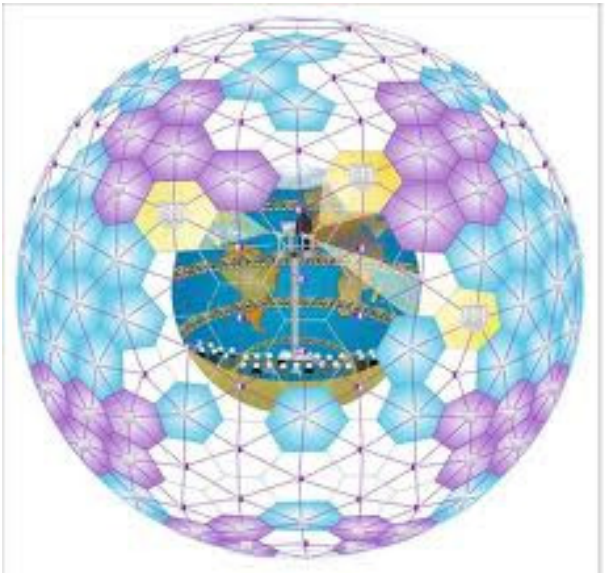
Some other interesting points, not explicitly developed in the [D6] deliverable, but evoked by (Quarantelli, 2000) concern:

- there is an accelerating focus in the civil protection area on using a generic or an all hazards approach,
- there is a growing emphasis on disaster mitigation to reduce the impact of disasters,
- the preparedness planning seems better than the response patterns.

This last analogy confirms the first assumptions explained concerning the fact that monitoring and warning systems could be good candidates for use-cases study. Some additional elements will confirm this strategic choice in the following lines. […] this can help in to the consideration of the future using of Grid technology in CP agencies. Finally, current research on a European organisation of CP agencies and data sharing policies should be a further motivation to design a standard infrastructure, such as Grid Technology.

One main difficulty which will be developed further concerns *the heterogeneous systems of civil protection agencies, organizationally complex and poorly integrated, both internally and externally*. For example, in France, each operational departmental centre develops its own operational systems and applications. However, current policies at national and European levels show a new trend to homogenise and centralise systems, applications and operations. Cyclops project follows this general trend.

7. The Future Internet service-oriented vision



7.1 The FP FIRE Initiative

(C31) The FP7 FIRE Initiative

Web Site / Document repository / Wiki: ict-fire.eu; cordis.europa.eu/fp7/ict/fire

Contractual documents:

Contact person: Piet Demeester (IBBT – UGent)

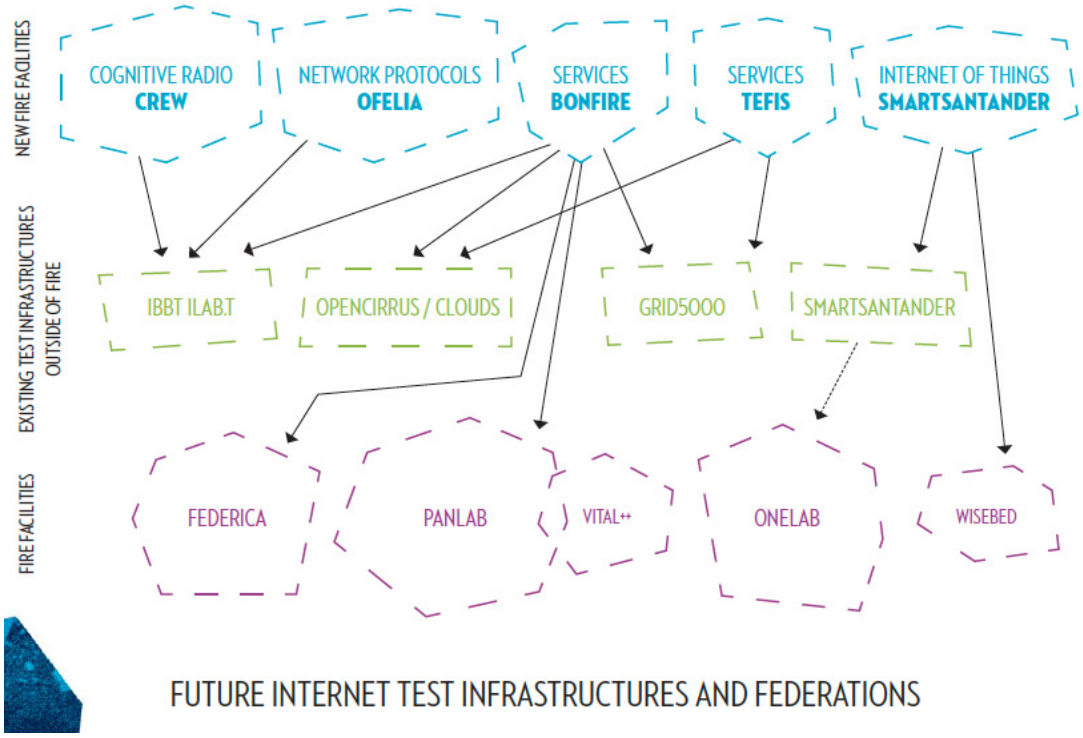
31a) Description of RI

Many researchers around the world have identified emerging limitations of the current Internet architecture and agree that it is time for research to take a fresh, long-term view re-consideration of the internet as a complex system, which cuts across layers from network connectivity to service architectures. This system-level approach calls for strategic, multidisciplinary research on new Internet concepts, including 'clean slate' or 'disruptive' ones. In order to measure, compare and validate scientific results and also to provide a

realistic basis for a scientifically rigorous impact assessment at technological, economic and social levels, these new paradigms need to be tested on a large scale. Issues at stake are for example: the balance between intelligence in the core versus in the edges; network neutrality and the end-to-end principle; the integration of network, compute and services infrastructures; trust and security by design; and the use of open source and open standards.

For this kind of 'experimentally-driven research' related to the *Future Internet*, researchers need an experimental facility for validating innovative research and developments on network and service architectures and paradigms. History has shown that many phenomena are only discovered when systems are deployed in 'real-life' situations. For instance, experimentally-driven security research should include experimentation with intentionally and unintentionally misbehaving programs and machines in a large, heterogeneous, real world-like testbed environment, which is nevertheless isolated from the outside world. Such experiments need to be conducted in a planned, controlled, responsible and legal manner. An experimental facility on Future Internet technologies must broadly support research on networks and services, in order to compare current and future approaches. Practical experiments are needed to give credibility and raise the level of confidence in the research finding. Furthermore, the experimentation must be performed at a large scale to be representative, convincing, and to prove the scalability of the tested solution. Experimental facilities based on federating testbeds at different levels of maturity, from proof-of-concept to validation, are needed to test compatibility, interoperability and to derive potential migration paths for innovative technologies.

To carry out experimentally-driven research on the Future Internet, researchers need a testing facility to validate their analysis of networks, service architectures and paradigms. FIRE addresses rising expectations of the Internet by providing a research environment for investigating and validating highly innovative and revolutionary ideas. This environment is called the FIRE Facility and it consists of several FIRE projects that are developing an experimental facility for open use. Each project develops a large-scale testbed or a federation of testbeds, which they contribute to the common FIRE Facility offering. The following pages give a deeper insight into the offerings of FP7 Objective 1.6 Call 2 FIRE Facility first-wave projects, which are now sufficiently mature for use: OneLab2 (OneLab experimental facility), PII (Panlab), FEDERICA, WISEBED and Vital++. These are the pillars of the FIRE facility, forming the framework on which the second wave of FIRE facility projects will be built. This second wave includes projects such as BonFIRE, CREW, OFELIA, SmartSantander and TEFIS which will form links with both existing FIRE facilities and test infrastructures outside of FIRE, these will be mature enough for use in 2011. These future relationships are illustrated in the figure below.



31b) PA/NC collaboration explanation

The FIRE initiative is part of the FP7 program. Integrated Projects (IP) will run for two to three years in order to develop experimental infrastructure and to open it up to potential users. There are no direct links to local *Public Authorities*. The *National Champions* may be part of the projects and may bring in their infrastructure to be further developed and used. An example is the iLab.t[25] of IBBT that is used in three IP projects (Crew, Ofelia and Bonfire). Another example is Grid500 in France[26].

31c) Budget, funding model, economic sustainability

The funding rules are typical FP7 funding rules. A project is (partly) funded by the European Commission (e.g. for universities: 75% is paid by the EC of 1.6 times the personnel budget).

The projects receives a budget that is split into three parts:

- 60%: this component is to support the planned developments and to 'benchmarking' some experiments. This component is not intended for research.
- 20%: FIRE Components – an operational prototype facility should be provided at an early stage in the project. Normally, at least 20% of the resources should be earmarked for gradually expanding the functionality of the prototype in a demand-driven and open way by federating testbeds and providing additional functionality within the facility.

[25] See: www.ibbt.be/en/ilab/ilab-t.
[26] See: www.grid5000.fr.

- 20%: FIRE Users – using the mechanism of open calls, it is expected that a further 20% of the resources are used for extending the use of the experimental facility for research groups that propose innovative usage scenarios exploiting the multiple dimensions and scale of the facility. These activities should exhibit a high degree of innovation in the use of the Facility, including system level experiments making a comprehensive use of several components of the facility, large scale experimentation, broad involvement of user communities, and assessment of socio-economic and other non-technological aspects. The results, lessons learnt and recommendations drawn must be of mutual interest, serving the needs of the users as well as helping the Facility operators to refine the concept of 'open coordinated federation of testbeds' and the services provided by the Facility. Support of individual experiments should be focused on the setting up and running of the experiment and should typically not exceed EUR 200,000 per experiment.

The total budget of the two calls was approximately 40 to 50 M€. There is one last call in early 2012 for an IP project (with the main focus on federation).

The *sustainability of the infrastructure is a major concern* that is addressed by the different projects but also within the coordination action Firestation (see below). This is 'work in progress'.

The EC is funding the projects for a period of typically three years but after that period, the availability of the infrastructures – outside the owner(s) – is based solely on the 'goodwill' of the owner(s). There are different options for sustainability:

- continuation in a new EC project (this is often difficult and uncertain),
- continuation on a (semi-)commercial basis (this is sometimes not allowed because of unfair competition),
- continuation based on national funding (the research institutes hosting the infrastructure get national funding),
- a combination of the above.

It is also important to understand that the FIRE infrastructure has to evolve over time because of technological evolution. This requires continued support in order to do further research on Future Internet experimental facilities.

31d) Governance / Management

All the projects have their own management structure (typical for EU projects). In addition there are some *Coordination and Support Actions* (CSA): Firestation is the main CSA for FIRE and in addition there are some more specific CSA's: FireBall, MyFire and Paradiso2.

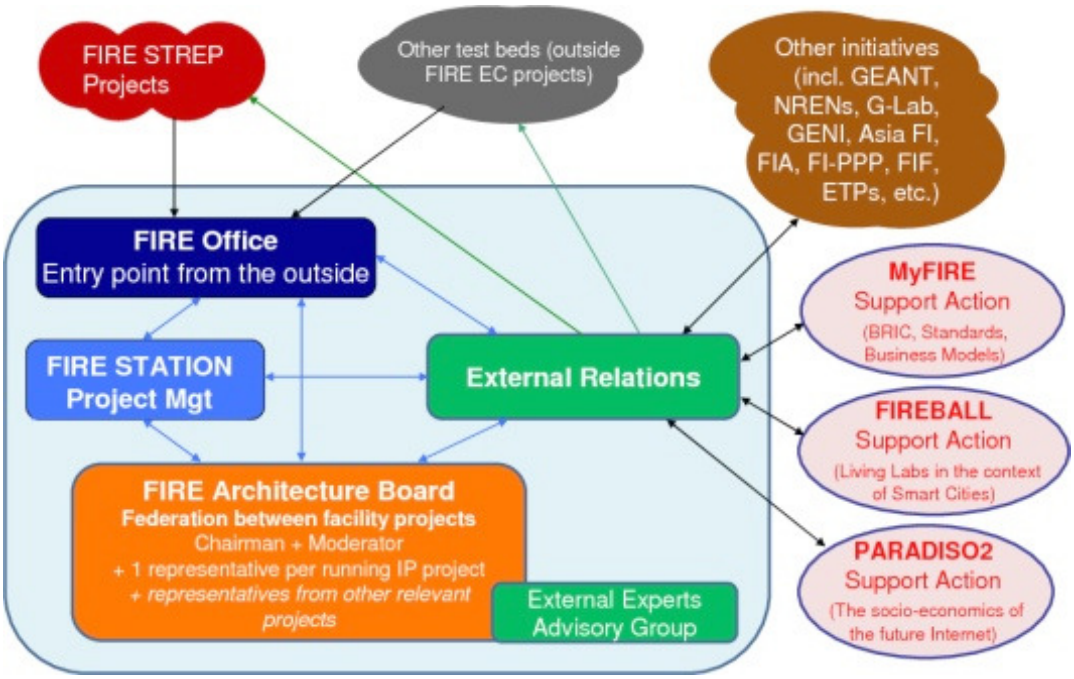
A short description of their goals is given below:

Fire Station: [27] FIRE STATION provides the FIRE Initiative with an active hub that matches, guides and co-ordinates demand for – and offering of – experimentation facilities in the context of future networks and services. The heterogeneous and modular field of *Future Internet Research and Experimentation* with its national and international stakeholder groups

[27] See: http://ict-fire.eu.

requires information sharing, cohesion building, community building and a single point of contact to co-ordinate and promote the FIRE approach with respect to the main requirements:

1) facilities need *synchronization*, *resource optimization*, and common efforts in order to offer customers the best possible *service* and ensure *sustainability* beyond project life times;
2) researchers need *correct and timely knowledge* about the available resources, *easy access*, *high usability* and appropriate *tools* to run and monitor their experiments.



FIRE STATION contains a *FIRE Office* and a *FIRE Architecture Board*. The FIRE Office serves as the single contact point and mediator when looking either for the right experimental resources or new customers for the facilities. The FIRE Architecture Board involves all FIRE facility builders in jointly deciding on the strategy and means to co-ordinate and facilitate the development of FIRE facility offerings to support the evolving needs of the customers. FIRE STATION increases the global collaboration between relevant stakeholders, promotes experimentally-driven approaches in future internet research and intensifies the usage of experimental facilities, ultimately speeding up the development process of new systems and services. The purpose of FIRE STATION is to join forces to allow for the most efficient bilateral (and multilateral when and if appropriate) collaboration, reduce duplication of work, share experiences and best practices and work for the future of Future Internet experimental research.

FireBall:[28] FIREBALL establishes a coordination mechanism through which a network of *Smart Cities* across Europe engage in long term collaboration for adopting *User Driven Open Innovation* to explore the opportunities of the Future Internet. The coordination process will

[28] See: www.fireball4smartcities.eu.

be grounded in exchange, dialogue and learning between Smart Cities, who are considered as key demand-side drivers of Future Internet innovation. It will also be grounded in bringing together the *Future Internet*, *Living Labs* and *Smart Cities* constituencies.

MyFire:[29] As part of FIRE, the challenge for the project MyFIRE is to develop the use of experimental facilities in Europe, in particular by increasing awareness of testing related best practices. The project will ensure a balance between the requirements for researcher's collaboration and the stakeholder's expectations. This means achieving good experimental activities, developing the sustainable testing methodologies and paying specific attention to the contribution to European standards development. The framework will be developed through the creation of open dialogue between the ICT networking research communities and experts from key areas of sociology, policy making, economic models and standard.

Paradiso2:[30] The PARADISO initiative, launched during the first half of 2007 (before the present financial and economic crisis) by Sigma Orionis and the Club of Rome, has been exploring the paradigm shift in global societal developments and the role that *Information and Communication Technologies* (ICT) could play in this envisioned future. PARADISO is an acronym formed by the two words PARADIgm and SOcietal, and an obvious reference to a better world.

The main activities during the period 2008-2009 consisted of the organisation of open events (including a high-level conference in Brussels in January 2009) and the release of first reference documents. These had an important impact as they appeared quite visionary and timely just at the time that the present worldwide crisis started to expand. During the period 2010-2011, PARADISO activities have been further exploring how might or should our societies evolve in the next decades and how can ICT, and the Future Internet in particular, contribute to making this future better.

31e) Countries and international collaborations

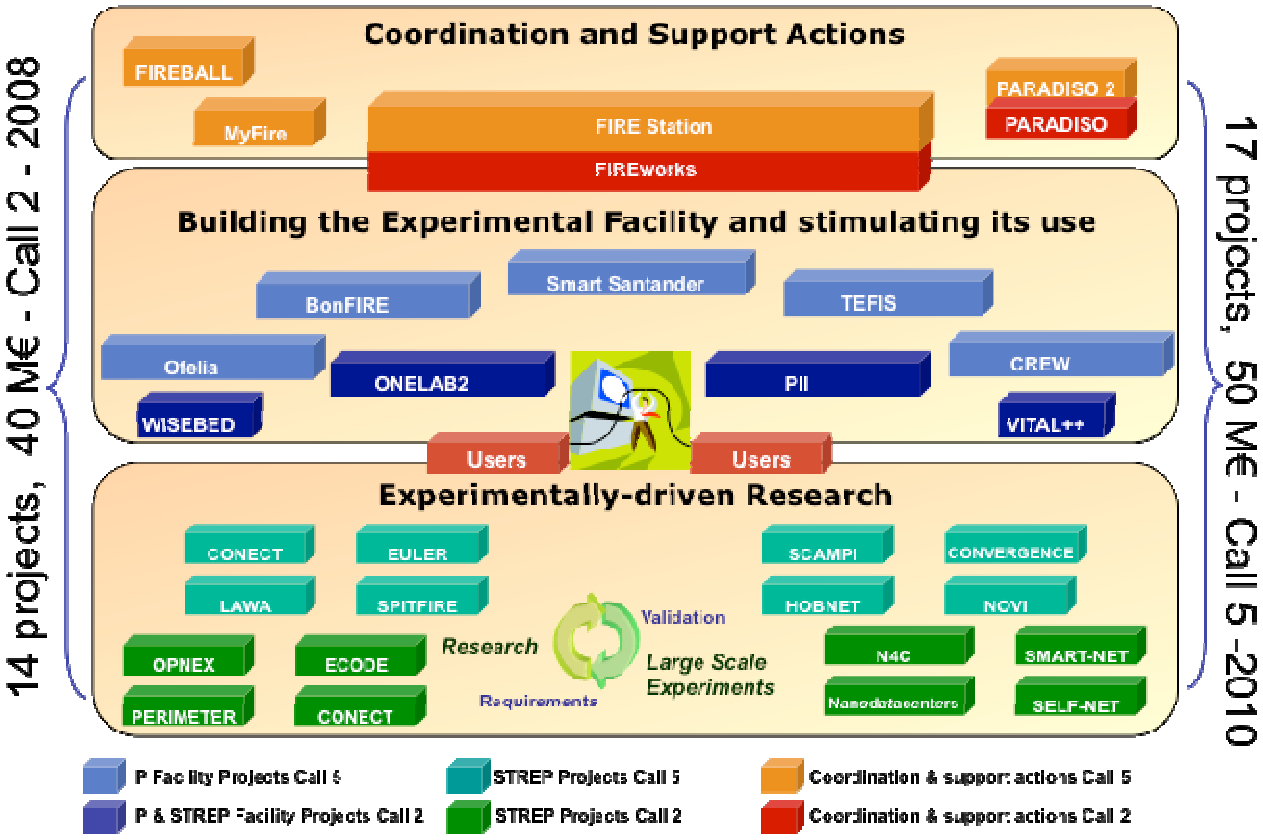
The FIRE infrastructure (IP[31]) projects bring together a number of important players in the field from different countries: including universities, research institutes, research networks and companies. The infrastructures are open to the research community in Europe (depending on certain restrictions such as capacity of the facility, novelty of the experiments, ...). There is also a strong push towards intercontinental collaboration on research infrastructures (US, Japan, BRIC countries, ...).

31f) History and evolution

The FIRE projects started in 2008 with a first wave of projects: Fireworks (CSA), OneLab (IP), PII (IP), Wisebed (IP) and Vital++ (STREP[32]). In a second wave, five new projects started in 2010, these were all IP's (Bonfire, Smart Santander, CREW, Ofelia and Tefis. In addition there are also research projects (STREP) on Future Internet and there were also 2 waves (in 2008 and 2010). In addition there is currently a third wave (two IP's and one NoE)

[29] See: www.my-fire.eu.
[30] See: paradiso-fp7.eu.
[31] IP: *Integrated Project*.
[32] STREP: *Specific Targeted REsearch Project*.

(January 2011) and a final call will result in projects starting in 2012. An overview is given in the figure.



31g) Security

Security is an issue that is identified in a number of projects and some projects have done some work in that area. There is presently no general view on it.

31h) Operations

One of the key challenges of FIRE is to work on the federation[33] of FIRE research infrastructures. Within the projects there has been work on the federation of testbeds provided by different partners, however between the projects, federation is still limited. Currently there is ongoing work to establish how useful federation is (in some cases it is, in other cases it is not) and how it could be realized. One of the challenges is the fact that in many cases different management frameworks are used.

[33] *Federation* could have different meanings ranging from *very close integration of facilities to loose interworking* or *easy access* using a single portal.