SEVENTH FRAMEWORK PROGRAMME
Research Infrastructures

INFRA-2010-2.3.1 – First Implementation Phase of the European High Performance Computing (HPC) service PRACE

PRACE-1IP

PRACE First Implementation Project

Grant Agreement Number: RI-261557

D6.1
Assessment of PRACE operational structure, procedures and policies

Final

Version:	1.0
Author(s):	Axel Berg (SARA)
Date:	23.06.2011

Project and Deliverable Information Sheet

PRACE Project	**Project Ref. №: RI-261557**	
	Project Title: PRACE First Implementation Project	
	Project Web Site: http://www.prace-project.eu	
	Deliverable ID: D6.1	
	Deliverable Nature: DOC_TYPE: Report	
	Deliverable Level: PU	**Contractual Date of Delivery:** 30 / June / 2011
		Actual Date of Delivery: 30 / June / 2011
	EC Project Officer: Bernhard Fabianek	

- - The dissemination level are indicated as follows: **PU** – Public, **PP** – Restricted to other 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).

Document Control Sheet

Document	**Title: Assessment of PRACE operational structure, procedures and policies**	
	ID: D6.1	
	Version: 1.0	**Status:** Final
	Available at: http://www.prace-project.eu	
	Software Tool: Microsoft Word 2003	
	File(s): D6.1.docx	
Authorship	**Written by:**	Axel Berg (SARA)
	Contributors:	Guillermo Aguirre de Cárcer (BSC), Gabriele Carteni (BSC), Liz Sim (EPCC), Jules Wolfrat (SARA)
	Reviewed by:	Norbert Meyer (PSNC), Florian Berberich (FZJ)
	Approved by:	Technical Board

Document Status Sheet

Version	**Date**	**Status**	**Comments**
0.1	18/04/2011	Draft	Outline
0.15	09/05/2011	Draft	Revised outline
0.25	24/05/2011	Draft	First text input by Axel
0.35	31/05/2011	Draft	Contributions by Jules, Guillermo, Gabriele
0.4	05/06/2011	Draft	Contribution by Liz, first complete draft except Exec summary and conclusions. First

			editorial revision by Jules and Axel
0.7	13/06/2011	Draft for PRACE internal review	Contributions by Axel, Liz, Guillermo, Gabriele and Jules
1.0	23/06/2011	Final	Final version, comments from internal PRACE review processed

Document Keywords

Keywords:	PRACE, HPC, Research Infrastructure, Operations, Service Catalogue, User support, Procedures, Policies, Security forum

Copyright notices

Table of Contents

List of Figures

List of Tables

References and Applicable Documents

[1] PRACE Project: http://www.prace-project.eu
[2] TeraGrid project: https://www.teragrid.org/
[3] EGI: http:www.egi.eu
[4] MAPPER Project: http://www.mapper-project.eu/
[5] PRACE Preparatory Phase Deliverable D4.1.4 Deployment of software stack to all prototype sites and selected tier-1 sites
[6] PRACE Preparatory Phase Deliverable D4.3 Specification document for PRACE systems management
[7] BSCW - Basic Support for Cooperative Work: http://public.bscw.de/
[8] TWiki: http://twiki.org/
[9] Subversion: http://subversion.apache.org/
[10] Trac: http://trac.edgewall.org/

List of Acronyms and Abbreviations

AAA	Authorization, Authentication, Accounting
AISBL	Association Internationale à But Non Lucratif
AUP	Acceptable Use Policy
BSC	Barcelona Supercomputing Center (Spain)
BSCW	Be Smart Cooperate Worldwide – groupware for efficient team collaboration
CA	Certification Authority
CEA	Commissariat à l'Energie Atomique (represented in PRACE by GENCI, France)
CERT	Computer Emergency Response Team
CINECA	Consorzio Interuniversitario, the largest Italian computing centre (Italy)
CMS	Content Management System
CSC	Finnish IT Centre for Science (Finland)
DART	DEISA Accounting and Reporting Tool
DEISA	Distributed European Infrastructure for Supercomputing Applications. EU project by leading national HPC centres.
EC	European Commision
EGI	European Grid Infrastructure
EPCC	Edinburgh Parallel Computing Centre (represented in PRACE by EPSRC, United Kingdom)
EUGridPMA	European Grid Policy Management Authority for Certificate Authorities issuing X.509 certificates for Grid or e-Science applications.
FZJ	Forschungszentrum Jülich (Germany)
GCS	GAUSS Center for Supercomputing
GEANT	the high-bandwidth, academic Internet serving Europe's research and education community
HLRS	High Performance Computing Center Stuttgart (Germany)
HPC	High Performance Computing; Computing at a high performance level at any given time; often used synonym with Supercomputing
ICM	Incident and Change Management
IDRIS	Institut du Développement et des Ressources en Informatique Scientifique, Paris, France
INCA	Grid monitoring software tool
ISTP	Internal Specific Targeted Project
LDAP	Lightweight Directory Access Protocol
LRZ	Leibniz Supercomputing Centre (Garching, Germany)
MAPPER	Multiscale APPlications on European e-infrRastructures
NOC	Network Operations Center
NREN	National REsearch Network
OGF	Open Grid Forum
OSG	Open Science Grid
PME	PRACE Module Environment
PFlop/s	Peta (= 10^{15}) Floating-point operations (usually in 64-bit, i.e. DP) per second, also PF/s
PKI	Public Key Infrastructure
PRACE	Partnership for Advanced Computing in Europe; Project Acronym
PRACE-1IP	PRACE 1st Implementation Phase
PRACE-2IP	PRACE 2nd Implementation Phase
PRACE-PP	PRACE Preparatory Phase Project

PRACE-TB	PRACE Technical Board
PSNC	Poznan Supercomputing and Networking Center (Poland)
RI	Research Infrastructure
RFC	Request For Change
SARA	Stichting Academisch Rekencentrum Amsterdam
SCI	Security for Collaborative Infrastructures
SNIC	Swedish National Infrastructure for Computing (Sweden)
SPG	Security Policy Group – EGI activity
SSH	Secure Shell
STFC	Science and Technology Facilities Council, UK
TFlop/s	Tera (= 10^{12}) Floating-point operations (usually in 64-bit, i.e. DP) per second, also TF/s
Tier-0	Denotes the apex of a conceptual pyramid of HPC systems. In this context the Supercomputing Research Infrastructure would host the Tier-0 systems; national or topical HPC centres would constitute Tier-1
TTS	Ticket Tracking System
UCL	University College London
UNICORE	Uniform Interface to Computing Resources
WP	Work Package

Executive Summary

The goal of this report is to present the work that has been done on the establishment of an organisational structure coordinating the technical operations of the PRACE distributed research infrastructure, including operational procedures and policies.

We have defined and established an operational management structure with Tier-0 site representatives and service category leaders that take part in the PRACE Operational Coordination Team. We have also established the PRACE Security Forum as well as an PRACE CERT team for operational security.

To support a good and complete overview, description and classification of PRACE Operational services, we have developed a PRACE Service Catalogue. This will serve as an important reference document within PRACE for service provision and will also be a starting point for definition and synchronisation of service levels and quality assurance and quality control.

We have setup a number of collaborative tools to support communication, collaboration and information sharing within PRACE, i.e. BSCW, TWiki and Subversion.

Assuring and maintaining a high and sustainable level of service provision requires good operational procedures and policies. We have setup procedures for incident management and change management. For change management we have defined various procedures for minor changes and major changes, the latter both for existing services and the deployment of new services.

We have developed a model for effective provisioning of user support, which is based on central point of entry (PRACE Helpdesk) for the users and effective and fast local management by the respective hosting partner.

Close collaborations on the operational level has been effective with DEISA2. Initial contacts with other projects like EGI, TeraGrid and MAPPER have been established.

1 Introduction

The presentation and delivery of the PRACE services to its users as a single coordinated distributed research infrastructure allows users to use the PRACE infrastructure as seamlessly as possible. To establish and assure this, coordinated actions are required on many different levels, from peer review and training activities to service deployment around the actual use of the infrastructure. Work package six (WP6) deals with the coordination of the technical operations and the technical evolution of the distributed PRACE infrastructure.

In this deliverable D6.1, the activities and results are described of the first year of task T6.1 ('coordination of the technical operations of the distributed RI') on the definition and implementation of an organisation structure for the technical operations of the distributed infrastructure, including common services and tools, user support, security policies and operational procedures and policies.

The challenge has been to define, coordinate and synchronise the common PRACE service activities, policies and procedures such that the PRACE infrastructure is operated as much as possible as a single distributed infrastructure while maintaining and acknowledging the local procedures, policies and common practices at the various hosting sites. This has been done through intensive discussions on the various topics among all partners in this work package to achieve common understanding and a common vision. In this first year of PRACE operations the focus has been on:

(1) defining and setting up an operational structure, policies and procedures;
(2) on the definition, classification and implementation of PRACE services as described in what is called the 'PRACE Service Catalogue', and
(3) on the development of a model for effective provisioning of user support.

From the hosting partners' site perspective, the focus has been on the integration of Tier-0 services, keeping in mind the DEISA2 services and integration of Tier-1 services next year in the context of the PRACE second Implementation Phase project (2IP).

The starting point for the work described in this report is threefold. First and for all the basis is the experience and best practices from HPC service provision of the individual HPC centres. Secondly, experience and best practices have been taken from the deployment of common and integrated operational services in the DEISA2 project. Many partners in this project have also been participating in the DEISA2 project, and collaboration took place with the DEISA2 coordinator of operations during this first project year. Thirdly, as a starting point for the list of common operational services that is being defined and deployed, the results were taken from the PRACE Preparatory Phase project, in particular from WP4 regarding the specification and deployment of the PRACE systems management software stack [5][6].

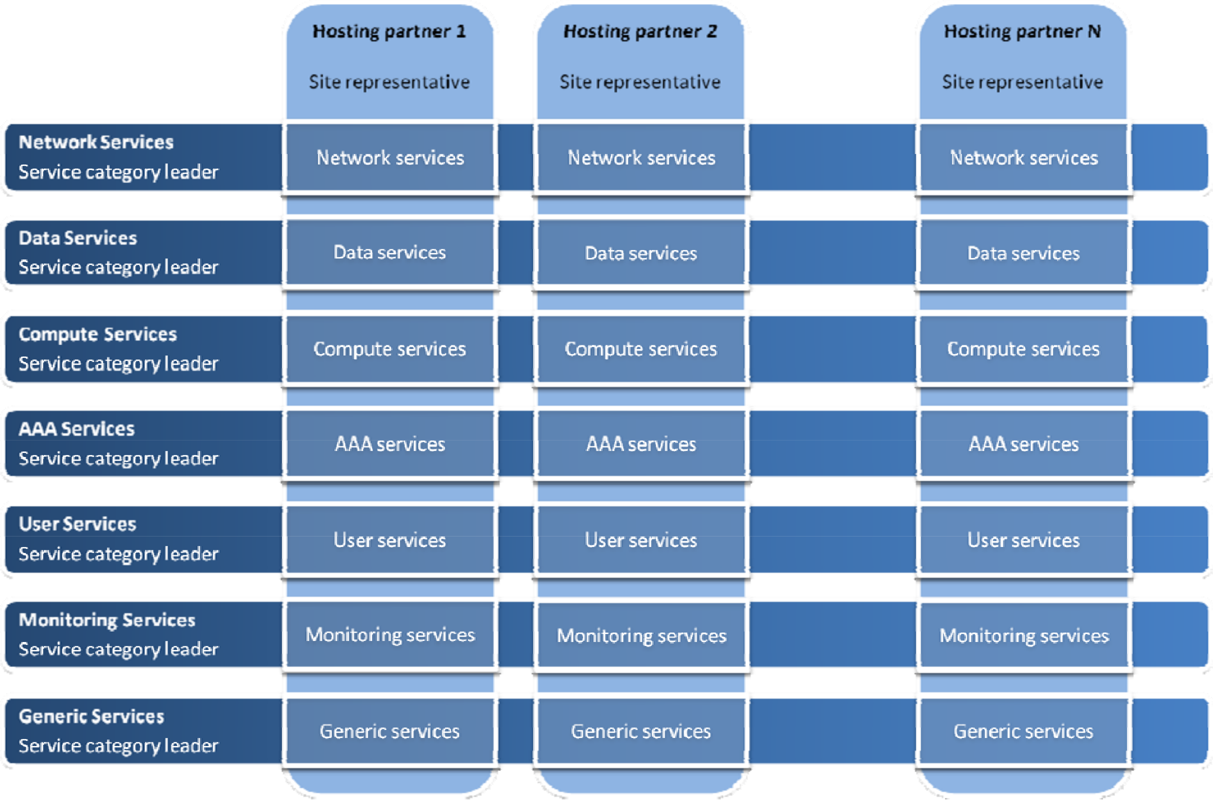
2 Operational structure and organisation

2.1 Operational structure & Operational Coordination Team

The PRACE distributed research infrastructure will be operated and presented to the users as a single research infrastructure, allowing the users to use PRACE as seamlessly as possible. This requires Tier-0 hosting partners to work closely together and synchronise service provision and service deployment as much as possible. On the other hand, PRACE services are deployed that provide a service layer that integrates the various hosting partner Tier-0 services, and makes the PRACE infrastructure much more than just a collection of individual Tier-0 hosting partners and Tier-0 services.

With hosting partners on one hand (vertical axis), and PRACE integrative services on the other hand (horizontal axis), a matrix structure is one of the most obvious ways to organise the technical operations. A matrix structure has also been used to organise the DEISA2 operations, and has proved to be an efficient way of running the operations of such a distributed infrastructure. This also paves the way for a smooth integration of Tier-1 operations in the near future that will take place in the PRACE-2IP project.

The basic PRACE operational management structure that has been established is depicted in figure 1.



	Hosting partner 1 Site representative	Hosting partner 2 Site representative	Hosting partner N Site representative
Network Services Service category leader	Network services	Network services	Network services
Data Services Service category leader	Data services	Data services	Data services
Compute Services Service category leader	Compute services	Compute services	Compute services
AAA Services Service category leader	AAA services	AAA services	AAA services
User Services Service category leader	User services	User services	User services
Monitoring Services Service category leader	Monitoring services	Monitoring services	Monitoring services
Generic Services Service category leader	Generic services	Generic services	Generic services

Figure 1: PRACE operational management structure

In this PRACE operational management structure, every Tier-0 hosting partner is represented by a so-called ‘site representative’. This site representative is responsible for the deployment and the status of the PRACE services at the hosting site, and is authorized to take operational decisions on behalf of the site. Currently for the Tier-0 sites that have deployed or will deploy their Tier-0 system in the near future (2011), the following site representatives have been appointed:

- GCS@FZJ:	Jutta Docter
- CEA:	Patrice Lucas
- GCS@HLRS:	Thomas Bönisch

For the organisation of the PRACE services, a number of different service categories have been defined, each with a responsible service category leader. Task 6.2 has been organised in such manner, that each service category has been organised as a separate subtask, and as a consequence each service category leader is subtask leader for a particular service category. The following seven service categories have been defined (in parenthesis the corresponding service category leader):

- Network services	(Ralph Niederberger, GCS@FZJ)
- Data services	(Frank Scheiner, GCS@HLRS)
- Compute services	(Gabriele Carteni, BSC)
- AAA services	(Jules Wolfrat, SARA)
- User services	(Denis Girou, IDRIS, Liz Sim, EPCC)
- Monitoring services	(Ilya Saverchenko, GCS@LRZ)
- Generic services	(Gabriele Carteni, BSC)

Details about the services that are deployed within the various service categories can be found in deliverable D6.2 ‘First annual report on the technical operation and evolution’.

The site representatives and service category leaders take part in the PRACE Operational Coordination Team. This team is lead by the WP6 leader (Axel Berg, SARA), and is complemented by representatives of other partners that provide PRACE services, and by the leader of DEISA2 Operations (Jules Wolfrat, SARA) to ensure synchronisation and anticipated merging in the PRACE-2IP project between PRACE (Tier-0) operations and DEISA2 (Tier-1) operations.

The PRACE Operational Coordination Team meets bi-weekly by tele/videoconference and held its first meeting on November 30, 2010 (milestone MS61). During the meeting the status and changes of all Tier-0 services and the status and changes of all PRACE services are discussed. Minutes of all meetings are made and are published on the PRACE BSCW pages.

2.2 PRACE Service Catalogue

The PRACE distributed research infrastructure is well on its path to provide a complete set of services to its users. Service provision to users is currently done jointly by the PRACE AISBL which has contracted the Tier-0 hosting partners by means of the Contributors Agreement and some specific third parties for the provision of specific services (e.g. provision of peer review tool), and by the PRACE-1IP project [1] by means of the project contract with the EC (see also Figure 2).

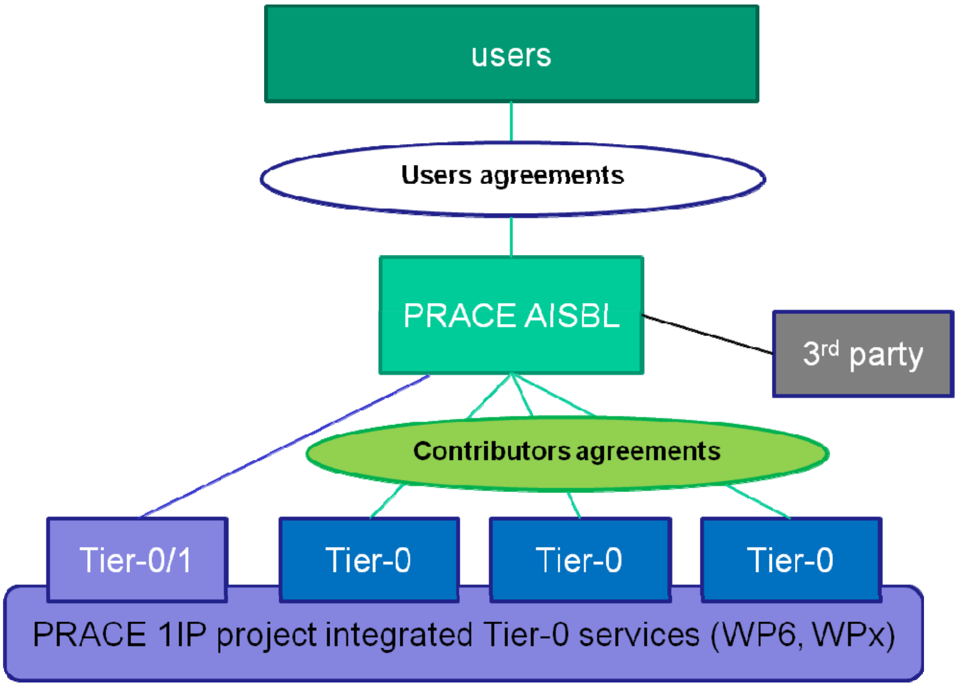


Figure 2: PRACE Service provision scheme and agreements

To support a good and complete overview of all PRACE Operational Services, we have started to develop what we call the PRACE Service Catalogue, which lists and describes the complete set of operational services that the PRACE RI is providing, from the point of view of PRACE as a service provider.

The current version of the PRACE Service Catalogue focuses on the Tier-0 services, Tier-1 services will be added later. The purpose of the PRACE Service Catalogue is:

- To describe all PRACE operational services
- To define PRACE service categories, and classify all PRACE services accordingly

In this way it describes the full PRACE service picture from hosting partners, other partners, the project and the PRACE AISBL.

An important aspect of the PRACE Service Catalogue is the classification of services. We have defined three service classes: Core services, Additional services and Optional services. The availability and support for each of these service classes is defined and described in Table 1.

Core services	
Availability:	Robust, reliable and persistent technologies that must be implemented and accessible at all PRACE Tier-0 sites, or provided centrally.
Support:	Support for these services is provided during support hours, i.e. the normal working hours according to the usual working arrangements of the particular Tier-0 site.

Additional services	
Availability:	Robust, reliable and persistent technologies that must be implemented and accessible at all PRACE Tier-0 sites where possible. Reasons for the service not being implemented at a Tier-0 site include technical, legal, and policy limitations, whenever an unreasonable effort is needed to provide the service.
Support:	If applicable, support for these services is provided during support hours.

Optional services	
Availability:	Implemented optionally by PRACE Tier-0 sites. Availability and long-term support are not guaranteed by PRACE.
Support:	PRACE RI provides support for these services on a case by case basis, in addition to any support provided directly by the specific site.

Table 1: Classification of PRACE Services as part of the PRACE Service Catalogue

Every PRACE service will be sorted according to this classification. It should be noted that the service classes define the availability of the services at the hosting sites, and are not related to service levels.

The definition of the services in the PRACE Service Catalogue is achieved through six criteria:

- **Description**: A brief summary of the service, indicating its value and a general overview of its implementation.
- **Class**: Services are arranged according to their expected availability and support across PRACE hosting partners. This classification is composed of three levels that indicate how essential a service is for the PRACE RI: Core, Additional, and Optional.
- **Provider**: The person(s), group(s), site(s), or team(s) involved in and responsible for the correct implementation and operation of the services.
- **Reference**: Documents and agreements that contain more specific details and information concerning the service provision.
- **Category**: Services are grouped into seven different categories, according to their specific domain: Compute, User, Data, Generic, AAA, Network, and Monitoring.
- **Software**: Concrete software products that have been chosen to implement the service.

The PRACE Software Catalogue will be regularly updated to document the actual status of all services and will be maintained as a living document, where all changes in services and their provision will be indicated. Status of services can change when new services are deployed, when levels of services are changed, when new service providers (i.e. new hosting partners) are integrated or when new software products are released. The document will at all times reflect the current situation of PRACE services, so that it can be used as the main reference document for service provision within PRACE.

The current version of the PRACE Service catalogue can be found in Appendix A of this document. The basis for the list of services in the PRACE Service catalogue has been established in the PRACE-PP in WP4[5][6].

The PRACE Service Catalogue is currently agreed on by all partners within WP6. The PRACE Service Catalogue will be discussed at the end of June 2011 within the PRACE Technical Board for feedback and further improvements. Successively the PRACE Service catalogue will require approval by the PRACE Management Board and the PRACE AISBL.

2.3 PRACE Security Forum

The establishment of the PRACE Security Forum was accepted at the end of the PRACE-PP project. The implementation started in the summer of 2010 with the acceptance by the PRACE-TB of a document which describes the objectives, the tasks and the organisation of this body. Three subtasks have been defined:

1) A Policy and Procedures task with the objective to implement “A trust model that allows smooth interoperation of the distributed PRACE services”. Activities of this task are
   a) The development of a “Statement of minimal security requirements”;
   b) To define and implement an Audit procedure;
   c) The review of policy documents (Acceptable Use Policy (AUP), user administration (AuthZ), incident response etc.);
   d) Representation in security related activities – EUGridPMA, OGF, SCI, SPG (EGI);
2) A Risk Review task with the objective to define and maintain “An agreed list of software and protocols that are considered robust and secure enough to implement the minimal security requirements”;
3) An Operational Security task with the objectives:
   a) To maintain and refine the procedures for incident handling;
   b) To investigate the use of intrusion tools in the infrastructure.

In addition the PRACE CERT is established, which operates under the responsibility of the Operational Security task. Members of the PRACE CERT team will in principle consist of members of partner CERTs.

A close collaboration with the existing DEISA2 security team existed from the start. There is a large overlap in partners and it is planned that both infrastructures will be fully integrated. For communication existing DEISA2 e-mail lists were used. In addition, a prace-security-forum e-mail list was established with all active members subscribed.

A face-to-face meeting was organized in October 2010 in Helsinki (milestone MS61). This was a shared meeting with the DEISA2 representatives. Two representatives from the EGI security activity were invited to strengthen the communication with this community and also to discuss the collaboration on policy and procedure topics. At this meeting the planning of activities for the three tasks and the assignment of responsibilities was discussed. The main topics were:

- Policies and procedures
  - One objective is to produce a repository of consortium partner IT security policies. Ralph Niederberger (FZJ) is leading this effort.
- Discussion of policy documents
  - Presentation of EGI SPG (Security Policy Group) activities by David Kelsey (STFC/RAL);
  - Discussion of the Acceptable Use Policy (AUP) document. A draft PRACE AUP is available as annex to the user agreement for Tier-0 users. This AUP differs from the DEISA version; the latter is almost similar to the EGI version.

It must be decided if for the future the PRACE AUP also will apply for access to Tier-1 resources or that a different AUP, based on the DEISA AUP will be used;

- It was agreed that a policy document describing the security obligations of a site also will be produced. This will be based on the PRACE contributor agreement for sites hosting PRACE services and examples of other infrastructures.

- Operational security – Discussion of the procedure for incident handling. Urpo Kaila (CSC) is leading this effort.

As a result of the meeting a list of decisions was published. The main progress since the meeting is:

- Feedback about the draft PRACE AUP is provided to WP2 as the responsible activity for the user agreement and the AUP;
- Several members of the Security Forum have been involved in discussions on a high level policy document for collaborating infrastructures "Security for Collaborative Infrastructures – SCI" in which several larger infrastructures are involved (EGI, TeraGrid, OSG,..);
- Security contact information is maintained and migration of all information, including e-mail lists, to the PRACE environment is in progress. Contact information with other infrastructures is exchanged for handling incidents which may affect more than one infrastructure (in several cases this proved to be very useful);
- PRACE is accepted as Relying Party (RP) of the EUGridPMA, which gives the opportunity to provide feedback on our needs and also to monitor the accreditation of new CA members and the audits of existing members;
- Operational security is a standard agenda item of the PRACE Operational Coordination Team.

2.4 Collaborative tools

Organising the PRACE Research Infrastructure requires a tight collaboration between partners throughout Europe. Although much of this collaboration is achieved through traditional means (face-to-face meetings, e-mail and videoconference), it is known from experience that specific tools are needed to support this collaborative process.

The main objective is to facilitate not only communication, but also the internal organisation and sharing of information and documents in real-time. For this purpose, three software tools have been chosen and have been set up accordingly: BSCW [7], TWiki [8] and Subversion [9].These tools have been setup and are deployed within this work package, but are generally available for the entire PRACE-1IP project and its partners.

An important aspect of the deployment of the PRACE collaborative tools is uniform access, in particular since these tools are serviced by different PRACE partners. Therefore access to all collaborative tools has been implemented through X.509 credentials to avoid both service providers and users of the tools to maintain username password combinations. BSCW (Basic Support for Cooperative Work) is a collaborative workspace software package developed by the Fraunhofer Society in the form of a web application. The server is hosted by FZJ at Jülich since the PRACE Preparatory Phase, and is accessible with credentials through a web browser. It supports among others document upload, event notification, and group management. This has been the default tool for document sharing throughout PRACE, and one can find deliverables (drafts and final versions), contact lists, calendars, and all other relevant documents for the project.

For information that is more dynamic and constantly evolving, it was decided to implement a wiki-based website that allows the creation and editing of any number of interlinked web pages via a browser using a simplified mark-up language. The specific software implementation that has been selected is TWiki, an open source wiki application that was first released in 1998. FZJ is hosting the TWiki application server, with X.509 certificate-based credentials for PRACE staff. A procedure for the registration of staff users was developed. The wiki is organised by Work Package and Tasks, with Work Package leaders and Task leaders in charge of the lower-level structure. The WP6 section includes work plans and status updates from Tier-0 sites implementing the PRACE Service Catalogue.

For the management of software development by PRACE staff a Subversion service has been set up. The service is integrated with a Trac [10] environment and hosted by SARA. It is mainly used by WP7 staff for the management of benchmark and application codes, but the service is available for other work packages for the distribution and management of software tools. Access is based on X.509 credentials and for the registration of users a similar procedure as for the wiki service is in use.

3 Operational procedures and policies

3.1 Incident and change management

Incident and Change Management (ICM) are two key activities for assuring and maintaining a high and sustainable operational level of the services provided by PRACE.

A correct definition and implementation of all steps taking part in these processes is the main objective of this activity. Like other operational procedures, which are shared and involve all partners, any solution should be focussed on efficiency and must respect the contributor and user agreements signed by the PRACE AISBL.

The current ICM procedures have been agreed on within this work package and are planned to be effectively in place at the start of Q3-2011.

3.1.1 *Incident Management*

The aim of Incident Management is to resolve any incidents causing an interruption of service in the fastest and most effective way possible. The required actions can be just restoring a service because of broken hardware or an in-depth analysis to the cause of the incident. In all cases it needs an efficient system for the tracking of these incidents. The procedure is tightly linked to the operation of the PRACE Service Desk, where incidents can be logged, analysed and solved as quickly as possible by using dedicated staff and tools (i.e., a Trouble Ticket System monitored by an incident team). In addition incidents can be handled locally at a site for more low level incidents, such as the replacement of a failing disk on a compute node. In any case any failure of a service which has an impact for the users must be logged and published in such a way that at least all staff is aware of the service break, but if possible also end users should be informed in some way. This kind of information can be published in the same way as that for scheduled maintenances.

At the time of writing, a model for the internal Service Desk is still pending for a final approval by all partners within the work package, but in principle incidents will be centrally logged, classified and then automatically routed to the hosting site, if they affect a particular instance of service on a specific Tier-0 system, or to the responsible site of a service category, if they affect a common service.

3.1.2 *Change Management*

In an infrastructure like PRACE with a high number of different, distributed and evolving resources and services, changes are abundant and a prominent factor to deal with. The purpose of a Change Management process is to manage those changes of services by respecting a clear and shared action protocol to achieve quality and continuity of the service at all times.

Within DEISA, a procedure for Change Management has been defined and implemented.

The change management procedure we describe below and that we use as a starting point for PRACE operations, is a revised and adapted procedure of what has been used in DEISA.

Sources of a request for change

In general, main reasons of a change are:

- Improvement of existing services;

- Introduction of new services;
- Meeting legal requirements.

In general for PRACE, changes are internally triggered by WP6, in particular, by Task 6.2 (Service operations) and Task 6.3 (Evolution of the infrastructure by deployment of new services).

Task 6.2 is responsible to undertake all deployment activities addressing PRACE integrative services, which are locally provided by Tier-0 sites and/or globally provided by PRACE. A change on the implementation of a service can be requested by a regular maintenance activity, which is the living part of any deployment process. Another example is a new software release.

The frequency of a “request for change” (RFC) on a production service depends on the underlying software and, in general, it can be high. High frequency types of changes have usually a minor impact.

Task 6.3 is the main source of changes on software since this activity is involved in the assessment and selection of new technologies. An RFC coming from this task is not frequent (each new technology has to follow several steps before going to production) but its impact can be significant on sites and users.

Change requests generated outside the WP6, will always be internally assigned and then formalized as RFC.

Type of changes

Definition of roles and responsibilities is a basic step for the creation of a well-defined process for Change Management. Depending on the type of a change, different roles and responsibilities are identified.

We have defined three types of changes: Minor, Major and Urgent.

A minor change is defined as an improvement of a service without a direct impact on providers (sites) and consumers (users). This type of change does not require a large coordination effort and does not have dependencies between partners. Moreover a fall-back plan should be easy. A common case for a minor change is a software update for achieving improvements on performance, stability and usability.

A major change of a service is defined as having a significant impact on sites and users. It requires an significant effort for coordinating required actions and for restoring the status of a service if the change process does not exit with success. Examples of major changes are software replacements, the introduction of new services, new user interfaces or new provisioning policies.

A change is defined urgent when it requires immediate action and has significant impact. Examples of urgent changes are fixing a security vulnerability or fixing a severe problem with a production service (i.e. the service can not be used anymore).

In this approach, we have assumed that any change requested by Task 6.3 (assessment of new technologies) should be considered as major since it is concerns the introduction of new services. Changes on production services always come from Task 6.2 and they could be major or minor. The table below gives an overview.

Source	Frequency	Type
WP6-T6.2	High	Major/Minor/ Urgent
WP6-T6.3	Low	Major

Table 2: Overview of types of changes in change management

Roles and responsibilities

The operational matrix structure adopted by WP6 allows an efficient and clear management of roles and responsibilities. Each service belongs to one of seven categories: data, network, compute, AAA, user, monitoring, internal.

For each service category a responsible person has been identified, both for Task 6.2 and for Task 6.3, and this person is the first in charge to define the type of a request for change.

The responsible person of each service category plays an important role in the change management process. Apart from the role to classify a request for a change, this person coordinates all the steps of the change management process and overseeing if changes are correctly implemented and reported on to task leaders and WP leaders.

Roles are also assigned to the PRACE Operational Coordination Team that is in charge of implementing a change, the PRACE security Forum that supervises all security issues the subtask User services that analyses the impact of a change to the PRACE users, last but not least, the proposer of a change that is generally a member of Task 6.2 or Task 6.3.

Following table summarizes roles and responsibilities.

Unit/Person	Role	Decision Level
Change Proposer	Propose a Request for Change	0
Service Category leader	Manage the Change Management process by assuring that partners correctly follow all defined protocols.	1
Task 6.2 Responsible	First level of approval for a request for change	2
Task 6.3 Responsible	First level of approval for a request for change	2
User Working Group	Verify the documentation attached to a request for change	2
Security Forum	Verify security issues on a request for change	2
WP Leader	Second level of approval for a request for change	3
Management Board	Third and final level of approval for a request for change	4

Table 3: Overview of roles and responsibilities in change management

Processes for Change Management

A common process is not applicable for any change. Change management has to fulfil different requirements, which are associated to each type of change (minor, major and urgent).

We have assumed that any change requested by Task 6.3 (assessment of new technologies) should be considered as major since it is responsible for introducing new services. Changes from Task 6.2 can be major, minor or urgent

Urgent changes have to follow a further dedicated approach to meet different needs, first of all a quick response in time.

We have currently defined four processes as part of the Change Management:

1. **Major Change proposed by WP6-Task 6.3**
2. **Major Change proposed by WP6-Task 6.2**
3. **Minor Change proposed by WP6-Task 6.2**
4. **Urgent Change**

All the steps included within each change process have to be logged.

Major Change from WP6-Task 6.3 (Introduction of a New Service)

STEP 1 (RFC Creation): The ISTP document (Internal Specific Targeted Projects), defined and adopted by T6.3 to log the evaluation of a new software/service, acts as input for a request for change.

The ISTP is managed and coordinated by the proposer of the new service/software, after a first approval by Task 6.3 leader, since the proposer should belong to one of the activities of Task 6.3.

Before processing by Task 6.2, which is responsible to deploy the proposed service, the ISTP has to include all following items:

- Reasons for the change and its impact to users and sites;
- Results of a test or certification procedure for the deployment of a new service;
- Information about installation and configuration;
- Security (all aspects about security have to be well documented);
- Monitoring (each service should be able to be monitored);
- Service Class (core, additional or optional);
- Migration Plan and Fall-Back Plan (if the introduction of a new service leads to the replacement of another one).

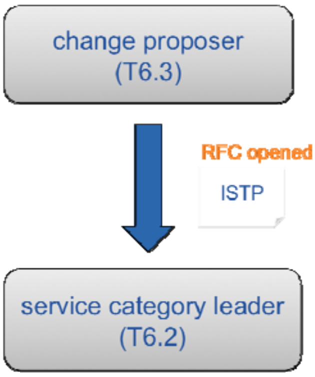


Figure 3: Scheme of Step 1 (RFC creation) in change management

STEP 2 (RFC Validation):

When the ISTP is received by the responsible of the deployment for a service category (Task 6.2), a validation step can start. First of all, it has to validate that ISTP contains all required information (STEP 1 successfully completed) and also that:

- Documentation is complete by referring to the User Working Group;
- Security issues are correctly handled by referring to the PRACE Security Forum;
- Monitoring is feasible by referring to the responsible for Monitoring Services;

Moreover, before to move the process into the deployment stage, the request for change has to receive the endorsement by Task 6.2 and WP6 leaders and the Technical Board.

If the validation is completed successfully, the service category leader announces the change in the PRACE Operational Coordination Team, which is in charge of the deployment.

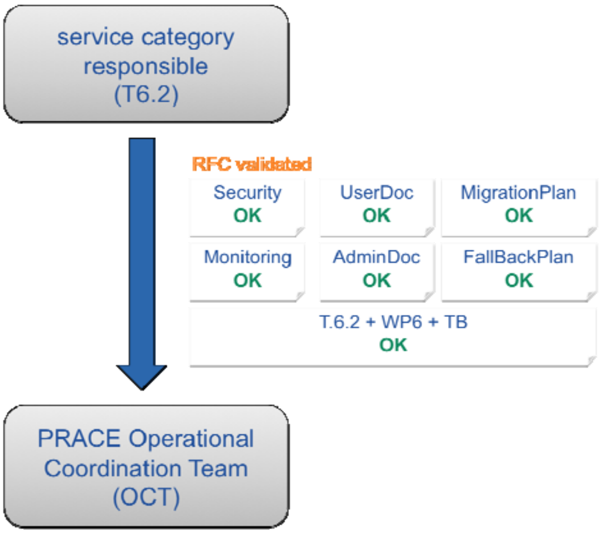


Figure 4: Scheme of Step 2 (RFC validation) in change management

STEP 3 (Deployment):

The PRACE Operational Coordination Team must be informed about the change: announcements must be sent to its mailing list and discussed in the regular bi-weekly PRACE Operational Coordination Team videoconference meeting.

If no objections are received the change can be planned. The period available for objections must be provided together with the announcement.

The service proposer and the service category leader should provide a timeline for putting the change in production.

This type of change cannot be rejected because it has been already approved by the TB. Only modifications on the timeline can be proposed.

STEP 4 (Closing):

The change will be closed by the service category leader after its successful implementation.

Major Change from WP6-Task 6.2 (Change on an existing service with impact on users and sites)

STEP 1 (RFC Creation): A major change proposed for a production service follows a different procedure since the service has been already tested and documented.

The request for change has to be documented without a strict protocol but it is essential to define the reason for the change and the impact for sites and users.

STEP 2 (RFC Validation):

The respective service category leader, starts a validation process by checking:

- The functional test of the proposed change;
- Green light from the User Working Group for the documentation;
- Green light from the PRACE Security Forum;
- Check if a fall-back plan is provided
- Communication to Task 6.2 and WP6 leader and to the Technical Board (specifying the impact of the change on sites and users)

STEP 3 (Deployment):

This step follows the same protocol of STEP3 for “Major Change from WP6-Task6.3”:

> *The PRACE Operational Coordination Team must be informed: announcements must be sent over the its mailing list and discussed in a regular PRACE Operational Coordination Team meeting.*
>
> *If no objections are received the change can be planned. The period available for objections must be provided together with the announcement.*
>
> *The service proposer and the service category leader should provide a timeline for putting the change in production.*
>
> *This type of change cannot be rejected because of it has been already approved by the TB. Only modifications on the timeline can be proposed.*

STEP 4 (Closing):

This step follows the same protocol of STEP3 for “Major Change from WP6-Task6.3”:

> *The change will be closed by the service category responsible after its successful implementation.*

Minor Change from WP6-Task 6.2 (Change on an existing service without impact on users and sites)

For a minor change a simplified procedure can be followed:

- The change must be documented;
- If a change in security policy is involved the PRACE Security Forum must agree with the change;
- The change must be announced to the PRACE Operational Coordination Team by e-mail at least three days before the date of implementation and preferably at least one week in advance;
- The change can be implemented if no objections are received;

- If objections are received a discussion must be planned in the regular meeting of the PRACE Operational Coordination Team.

<u>*Urgent Change*</u>

An urgent change is characterized as one that must be implemented as quickly as possible because it addresses security vulnerabilities and/or it fixes a severe problem with a production service.

For an urgent change a simplified procedure can be followed:

- The change is announced by e-mail and shortly documented by the Task 6.2 person in charge of the affected service;
- If no dependencies are in place, the change can be implemented immediately. Otherwise an urgent meeting has to be scheduled for coordinating the actions;

Tools

The wiki based website is used for logging changes.

There is a central table for each type of changes that is 4 tables, and links to wiki pages where details are provided.

BSCW document workspace is be used to upload ISTP and other related documents.

3.2 Security policies

Operational security policies for incident handling are based on the DEISA policies. Further improvements and extensions are discussed in the PRACE Security Forum. The basic assumption is that each site has adequate policies and procedures to manage local incidents. These have been presented by sites at a meeting of the security team of DEISA, February 2011, where also the current PRACE Tier-0 sites have presented their policies. These presentations are available for all partners.

Because of the integration of sites in the PRACE infrastructure it is important that a security incident at one of the sites is reported to the other partners of the infrastructure too. This is implemented by the PRACE/DEISA CERT team, which is a list of site contacts, the site CERT teams. Both phone numbers and e-mail addresses are provided. In case that it is clear that more than one site may be affected by an incident, video conferences can be scheduled within a couple of hours to discuss the measures to be taken. All necessary information is exchanged within the CERT team and all actions taken are reported by sites involved in the incident.

3.3 Model for user support provisioning

3.3.1 *Centralised PRACE Helpdesk*

The PRACE User support model, will consist of a centrally located but locally managed Helpdesk. *'Centrally Located'* - There will be a single entry point to PRACE for users to request support. A central PRACE Ticket Tracking System (TTS) has been installed at

CINECA to support this. All PRACE user issues will be routed to this system. *'Locally Managed'* - All support requests for support of a single Tier-0/Tier-1 system are handled directly by the Tier-0/Tier-1 hosting site, which have the right expertise to handle the support request. Support will be provided in accordance with the Contributors Agreement. Support for distributed services on the PRACE RI will be handled by the appropriate sub-team of WP6.

The guiding principles behind such an approach for User Support are:

- To present PRACE as a single distributed RI to users
- To be able to run statistics and analysis on all PRACE support requests, as information for the PRACE AISBL and to enable improvement of support on the PRACE level
- To serve support requests from users according to the service levels as contracted in the Contributors agreement between the Tier-0 hosting partner and the PRACE AISBL or as contracted between a hosting partner and its funding agency

User Support Interface

The primary support interface for PRACE users is via a web interface. PRACE users can request support through a web form published on the PRACE website. Access to the form is restricted to those PRACE users registered in LDAP. In this form users are obliged to indicate the PRACE system the problem or request is related to (obligatory pull down menu). Such requests can be automatically logged and processed centrally and rerouted directly without any delay to the Tier-0 hosting partner. In this way support response times can be guaranteed by the hosting partners. Such a system is scalable and will work irrespective of the number of hosting partners. The use of the web interface will be included in an online PRACE Primer document for all users.

A secondary email based interface is also available. It is possible that high level requests for information could be raised by individuals who are not yet registered PRACE users, or a registered user may encounter a problem with the web interface. A generic support email address support@prace-ri.eu would be available to support these use cases. Emails sent to this address would be routed to the PRACE TTS. These issues would then be routed manually to the correct team by the PRACE Helpdesk on Duty (detailed below).

In addition to the generic email address, we will also incorporate site specific email addresses. These would be configured to route tickets directly to the correct Tier-0/Tier-1 site queue within the PRACE TTS e.g. support-curie@prace-ri.eu. This is in response to concern that some users in some geographies are used to using email in order to gain support, and would not use the online web interface. If the users mailed the generic email address provided, support@prace-ri.eu, there would be a delay in the routing of the ticket as manual intervention is required to pass the ticket to the appropriate site. The concern is that the hosting site would then be unable to resolve the user issue in line with the service levels agreed in the Contributors Agreement. The addition of system specific emails detracts slightly from our primary principle of presenting PRACE as a single distributed RI, however users need only to be advised of the email address pertaining to the few site(s) they are using, and do not need to be given an extensive list of email addresses.

Internal Support Interface

Support staff will be presented with an extended view. Whereas a user will be given a selection of sites to choose from, internal support staff at hosting sites will also be able to associate trouble tickets to specific service queues. For example, a user may raise a problem at a Tier-0 site. The support staff at the Tier-0 site will triage the issue, and may find that it relates to a generic issue with a centrally managed service, such as the PRACE Modules

Environment (PME). Any fix or change to the PME would be outside the control of the Tier-0 site, and the ticket would be routed to the WP6 team responsible for the PME service.

PRACE Helpdesk on Duty

As part of the support process, a role has been developed that is called ‘PRACE Helpdesk on Duty’. The PRACE Helpdesk on Duty will rotate weekly among the PRACE operational partners. The tasks of the PRACE Helpdesk on Duty are:

- Regular inspection each working day of all emails which have been sent to the generic support email address of the TTS
- Forwarding of all such emails as tickets to the correct hosting partner or WP6 internal support team
- Monitoring the status of the queues and ensuring any exceptions or major issues are highlighted
- Handover this duty by means of a weekly report, including the status report on any generic trouble tickets

This role is very similar in nature to the PRACE Operator on Duty (as described in Section 3.4 below). As the primary user interface to the Helpdesk is via the web interface, the effort required to manually route tickets to the correct support queues is expected to be minimal. The PRACE operational partners may therefore choose to staff these two roles with the same resources in order to simplify the scheduling of effort.

3.3.2 *User Documentation*

In addition to the provision of a Helpdesk, clear and concise User Documentation is also required to be provided on the PRACE-RI website. Document owners will be assigned for each of the services defined within the PRACE Service Catalogue. In addition to the specific services, a basic PRACE Primer will also be published, providing users with a basic introduction to the services available including the PRACE support structure. The aim of the documentation is to provide clear and simple guides to permit users to exploit the PRACE distributed infrastructure to its full capacity.

Documentation on the usage of the PRACE document authoring environment will be provided for all document authors on the PRACE wiki.

It is vital that a process to ensure the quality and consistence of User Documentation must be adopted. A PRACE User Documentation Review Panel consisting of the main document authors, plus a representative from each PRACE Site will be formed.

Minor changes to documentation (such as typographical errors) may be made directly by the document owner. Any major changes (such as configuration changes or the introduction of additional services) will require the review of the Panel. The full details of the operation of the panel and the guidelines it must follow are yet to be finalised and will be published on the PRACE wiki.

Publishing of documents to the PRACE-RI website will be performed only by the person of WP3 responsible for the website or the User Services Sub-Task Leader within WP6.

3.4 Quality assurance and quality control

Quality assurance is the systematic monitoring and evaluation of services to maximize the probability that service levels are being attained by the service delivery process. Quality assurance and quality control are therefore important whenever services are delivered. In the PRACE situation the service delivery is complex as it is delivered as a ‘single’ PRACE service to the users, but actual service delivery is a combination of services provided by many hosting partners and other partners. In the process of defining quality assurance and quality control mechanisms and procedures, a number of prerequisite steps are necessary. These are (1) the definition and agreement of the set of PRACE services (so what services is PRACE going to provide), (2) the definition and agreement of the operational procedures and policies for the service delivery, (3) the definition and agreement of service levels for each of the services. All these steps are a prerequisite for the implementation of quality assurance and quality control.

Basic service delivery and resource provision by the hosting partners is contracted between the PRACE AISBL and the Tier-0 hosting members. The services and the corresponding service levels are described in the Contributors Agreement that is signed between each Tier-0 hosting partner and the PRACE AISBL.

For the integrative PRACE operational services that are subject of this work package, we are in the process of finalising and confirming agreement among all partners on the initial set of PRACE services that are delivered through this project. The current state of the work is described in the PRACE Service Catalogue paragraph. By the end of year one of this project we have also established a first set of common procedures and policies for service delivery (see paragraph on Incident and Change management). The next step in this process is the definition of service levels for each of the services which is planned at the start of year two of the project. This is an important but challenging process which requires intensive synchronization and tuning of service levels as well as common and best practices among all operational partners.

Of course some of the operational procedures and policies that are described in paragraph on Incident and change management are closely related to quality assurance, or are in fact procedures for quality assurance. Also the monitoring activities that have been developed and are implemented are a prerequisite for quality assurance. On top of that a quality assurance procedure has been developed that is called ‘PRACE Operator on Duty’. The PRACE Operator on Duty is rotated weekly among the PRACE operational partners. The tasks of the PRACE Operator on Duty are:

- Daily inspection of all PRACE monitoring information
- Ticket creation, ticket handling and monitoring
- Handover this duty by means of a report, including the status report on trouble tickets

The PRACE Operator on Duty will be implemented at the start of year 2, when the PRACE trouble ticket system is fully operational.

4 Collaboration and coordination with other e-infrastructures

4.1 DEISA2 and PRACE-2IP

Most DEISA2 partners are involved in PRACE-1IP activities too and in most WP6 activities many individual members are familiar with the DEISA2 environment. Especially for the integration of the Tier-1 infrastructure a close collaboration is important:

- The dedicated network provided by GÉANT and NRENs is shared between DEISA and PRACE-Tier-0 systems;
- GridFTP facilities provided by DEISA can be used by PRACE users too;
- The UNICORE infrastructure facilities are shared between the two infrastructures;
- The AAA services are based on the same tools;
- The Common Production Environment is based on the same principles, which gives the user a familiar environment for either Tier-0 or Tier-1 systems;
- Installation and configuration information for most services could be based on DEISA provided information;
- For operational procedures the DEISA examples were a good starting point.
- The results of evaluations by DEISA of new technologies were available for PRACE and could be used for further evaluation or preparation of a production service in PRACE.

In DEISA2 at the end of the project an inventory was made of actions needed for all services that should be integrated or migrated to PRACE as part of the migration to PRACE-2IP. This was also discussed in a meeting with PRACE partners in an internal meeting at Helsinki, right after the DEISA/PRACE symposium. A high level overview presentation was prepared of the requirements for a new Tier-1 site that will be integrated in the infrastructure.

As a result of the close collaboration the DEISA2 Tier-1 infrastructure is already highly integrated in PRACE and no big problems are expected with the integration of new Tier-1 facilities in the PRACE infrastructure.

4.2 Other e-infrastructures

4.2.1 *EGI*

A first exploratory meeting between the leader of the PRACE Operational Coordination Team (Axel Berg, SARA), the DEISA2 Operations leader (Jules Wolfrat, SARA), and EGI (EGI.eu director Steven Newhouse and Chief Operations Officer Tiziana Ferrari) [3] took place in Amsterdam at September 22nd, 2010. The purpose of the meeting was to exchange information, status of affairs on operations and future plans. The most important conclusions of the meeting were that (1) both organisations were just starting up or reassessing their operations and operational procedures and (2) concrete use cases would be very instrumental in concrete operational collaborations, synchronisations or even interoperations. We agreed that we would meet again after a year, when both organisations had clear operational procedures and policies in place that could be exchanged. We also agreed that we would both look for real use cases that require the use of both infrastructures.

For security related issues a close collaboration is already established, both for the exchange of information about security incidents and the discussion of security related policies and procedures.

4.2.2 *MAPPER*

The MAPPER project (http://www.mapper-project.eu/), which is an acronym for Multiscale Applications on European e-Infrastructures, will deploy a computational science environment for distributed multiscale computing on and across European e-infrastructures[4]. By taking advantage of existing software and services, as delivered by EC and national projects, MAPPER will result in high quality components for today's e-Infrastructures. In this project, a number of important and interesting scientific applications are present, that require both capability and capacity (grid) resources. In this sense these are a very good use case for collaboration and interoperation between the PRACE infrastructure and the EGI infrastructure.

On May 13, 2011 a joint MAPPER-PRACE meeting took place, with 7 representatives from PRACE from both WP6 (Operations and Technology) and WP7 (Applications). The purpose of this meeting was to exchange information, generate a common understanding and establish important personal contacts. For PRACE this meeting was also important to capture technical as well as user requirements from this distributed multiscale community. Also two representatives from EGI.eu joined the meeting.

The meeting has been very successful and a number of concrete actions have been commonly agreed:

- Collaborative actions: MAPPER proposed two applications (in-stent restenosis and nano material science) as first candidates to demonstrate distributed multiscale computing, also in an interoperable mode, coupling ‘prace-type’ systems (e.g. a Tier-1 system, with the same software stacks as PRACE machines at LRZ and SARA) with an ‘EGI-type’ machine (being resources from PL-Grid at PSNC) and a local machine (e.g. from UCL). A small joint team is setup to make and execute an plan to run those applications over the summer timeframe
- Technical requirements capturing: relevant technical MAPPER deliverables are shared with PRACE and will be screened for technical requirements. Feedback will also be send to MAPPER
- Petascale application requirements: MAPPER application requirements will be made more precise, and will be investigated if petascaling for selected applications is required, and how this could be established. Also the preparatory access could be a good way to prepare MAPPER applications for access to PRACE Tier-1 or Tier-0 systems.

4.2.3 *TeraGrid*

There have been informal discussions with John Towns, chair of the TeraGrid forum, about collaboration in operational topics between PRACE and TeraGrid [2]. It is anticipated that, starting July 2011, TeraGrid will migrate to the eXtreme Digital (XD) program. Based on their current experience they formulated as one of the objectives to implement more mature operational practices, with 1) increased focus on productivity and ease of use; 2) increased and enhanced security, reliability, and quality assurance. It will be interesting to exchange experiences and ideas on how operational practices can be improved.

5 Conclusions

The presentation and service delivery of the PRACE services to its users as a single coordinated distributed research infrastructure allows users to use the PRACE infrastructure as seamlessly as possible. To establish and assure this, coordinated actions are required on many different levels of service provision around the actual use of the infrastructure. The challenge in this first year has been to define, coordinate and synchronise the common PRACE service activities, policies and procedures such that the PRACE infrastructure is operated as much as possible as a single distributed infrastructure while maintaining and acknowledging the local procedures, policies and common practices at the various hosting sites. This has been done through intensive discussions on the various topics among all partners in this work package to achieve common understanding and a common vision. In this first year of PRACE operations we have been able to:

(1) establish an organisational structure coordinating the technical operations of PRACE, including the definition of operational policies and procedures;

(2) develop a 'PRACE Service Catalogue' that defines and classifies PRACE common services, and

(3) develop a model for effective provisioning of user support.

From the hosting Tier-0 partner site perspective, the focus has been on the deployment and integration of Tier-0 services.

Together we have been able to build a common and solid ground on many different and sometimes difficult issues around service provision by a set of hosting partners and common services in a distributed research infrastructure. This enables us to focus in the second year of the project on (1) operational integration of the second (CEA) and third (HLRS) Tier-0 systems; (2) improvement and further evolution of operational procedures and policies; (3) focus on quality assurance and quality control; (4) collaboration with the PRACE-2IP project on operational synchronisation of Tier-1 hosting partners and (5) intensify collaborations with other e-infrastructure projects like EGI, MAPPER and TeraGrid.

The set of common operational services across the Tier-0 systems and interoperability with and integration of Tier-1 systems (within the PRACE-2IP project) will ultimately become permanent and sustainable services within the PRACE Research Infrastructure.

6 Appendix A: PRACE Service Catalogue

Service Classes

Core services	
Availability:	Robust, reliable and persistent technologies that must be implemented and accessible at all PRACE Tier-0 sites, or provided centrally.
Support:	Support for these services is provided during support hours, i.e. the normal working hours according to the usual working arrangements of the particular Tier-0 site.

Additional services	
Availability:	Robust, reliable and persistent technologies that must be implemented and accessible at all PRACE Tier-0 sites where possible. Reasons for the service not being implemented at a Tier-0 site include technical, legal, and policy limitations, whenever an unreasonable effort is needed to provide the service.
Support:	If applicable, support for these services is provided during support hours.

Optional services	
Availability:	Implemented optionally by PRACE Tier-0 sites. Availability and long-term support are not guaranteed by PRACE.
Support:	PRACE RI provides support for these services on a case by case basis, in addition to any support provided directly by the specific site.

Service classes reflect the availability of a service at all Tier-0 sites, and are not related to service levels.

Uniform access to HPC	
Description:	Allows a user to execute code on PRACE Tier-0 systems, monitor its evolution and retrieve the results across Tier-0 systems.
Class:	Core
Provider:	Tier-0 site + WP6 (compute services representative of the PRACE Operational Team)
Reference:	User Agreement
Category:	Compute
Software:	UNICORE

Interactive command-line access to HPC	
Description:	Allows a user to connect remotely to a Tier-0 system and execute command-line instructions.
Class:	Core
Provider:	Tier-0 site + WP6 (compute services representative of the PRACE Operational Team)
Reference:	User Agreement
Category:	Compute
Software:	X.509-based SSH

Project submission	
Description:	Provides users with a centralized point for submitting projects for Peer Review.
Class:	Core
Provider:	PRACE Peer Review Team
Reference:	PRACE PP D2.4.2
Category:	User
Software:	PRACE Peer Review Tool

Data transfer, storage and sharing	
Description:	Each PRACE User is provided a “home” directory and access to a project space shared with his User Group, at each of the assigned Tier-0 sites. The amount of space in each of these directories is indicated in Annex A of the User Agreement. Data can be transferred to and from these directories.
Class:	Core

Provider:	Tier-0 site + WP6 (data services representative of the PRACE Operational Team)
Reference:	User Agreement, Contributor Agreement
Category:	Data
Software:	GridFTP (core) UNICORE

HPC Training

Description:	Provides training sessions and workshops for topics and technologies in high-performance computing, as well as online and offline education material.
Class:	Core
Provider:	WP3
Reference:	
Category:	User
Software:	

Documentation and Knowledge Base

Description:	User documentation in the form of an online knowledge base, including manuals and other information and tools that are indispensable for the users.
Class:	Core
Provider:	PRACE AISBL + WP6 + WP7
Reference:	
Category:	User
Software:	DocBook, CMS

Data Visualization

Description:	Converts data into images as a tool to help users with analysis.
Class:	Optional
Provider:	Specific PRACE sites
Reference:	
Category:	Generic
Software:	

Authentication

Description:	Confirm the identity of a user and bind that user to a new account. This

	involves identifying a user's certificate, creating a global PRACE RI account for the user on the central LDAP and making it available for distribution on all PRACE RI Resources.
Class:	Core
Provider:	Peer Review Team + Tier-0 site + WP6 (AAA services representative of the PRACE Operational Team)
Reference:	Contributor Agreement, PRACE Security Policy
Category:	AAA
Software:	PKI X.509-based SSH LDAP

Authorization

Description:	Specifies access rights for each user account created based on the content of the specific User Agreement and the PRACE Security Policy. Ensures that security rules and access rights are obeyed, and manages changes to these (based on new security policies or redefined User Agreements).
Class:	Core
Provider:	Peer Review Team + Security Forum + Tier-0 site + WP6 (AAA services representative of the PRACE Operational Team)
Reference:	User Agreement, PRACE Security Policy, PRACE Acceptable Use Policy
Category:	AAA
Software:	LDAP

Accounting

Description:	Keeps track of resource usage linked to an account for analysis by users and management. Guarantees that users are not exceeding their limits, as specified by their User Agreement.
Class:	Core
Provider:	Peer Review Team + Tier-0 site + WP6 (AAA services representative of the PRACE Operational Team)
Reference:	Contributor Agreement
Category:	AAA
Software:	LDAP DART backend

Information Management

Description:	Provides a common PRACE collaborative environment for sharing relevant

	information between PRACE sites (BSCW, wiki, subversion, ...).
Class:	Core
Provider:	WP6
Reference:	
Category:	Generic
Software:	BSCW, Twiki, svn

Network Management	
Description:	Establishes and maintains network connections between all PRACE nodes (Tier-0 and Tier-1 systems). The PRACE NOC operates the PRACE backbone network and the corresponding network monitoring system. The PRACE NOC coordinates networking activities of PRACE partners, who are responsible for creation and management of network connection between the local resources and the PRACE backbone. PRACE partner's local network specialists and the PRACE NOC should support PRACE users in using the PRACE network infrastructure. The PRACE backbone will be dedicated, whereas local site connectivity of HPC systems and PRACE servers to the global Internet are public.
Class:	Core
Provider:	PRACE NOC and local NOCs of PRACE partners (at least one person per site should be also a network services representative of the PRACE Operational Team)
Reference:	
Category:	Network
Software:	iPerf

Monitoring	
Description:	Periodically presents and analyzes up-to-date essential PRACE parameters and service availability to keep track of the situation of the distributed RI, for example: system uptime/downtime and usage levels, network connections, software and service availability, …
Class:	Core
Provider:	Tier-0 site + WP6 (Monitoring services representative of the PRACE Operational Team)
Reference:	
Category:	Monitoring
Software:	INCA iPerf

Reporting

Description:	Periodic reports of system utilization from the Tier-0 hosting partner to the PRACE AISBL.
Class:	Core
Provider:	PRACE AISBL + Tier-0 sites
Reference:	Contributor Agreement
Category:	Monitoring
Software:	DART

Software Management and Common Production Environment

Description:	Provides software, tools, libraries, compilers, and uniform mechanisms for software and environment configuration. Presents users with a uniform environment across PRACE Tier-0 systems, hiding inessential details such as software installation paths.
Class:	Core
Provider:	Tier-0 site + WP6 (tasks 6.2 and 6.3)
Reference:	
Category:	Generic
Software:	Modules

First Level Support

Description:	Each PRACE User has access to a centrally managed Helpdesk. Issues raised to the Helpdesk are routed to the appropriate First Level Support team. First Level support is responsible for gathering the user's information and determining their issue by identifying what the user is trying to accomplish, analyzing the symptoms and figuring out the underlying problem.
Class:	Core
Provider:	Tier-0 site + WP6 (User services representative of the PRACE Operational Team)
Reference:	User Agreement, Contributor Agreement, PRACE-1IP D6.1
Category:	User
Software:	RT-TTS

Higher Level Support

Description:	Provision of support above and beyond basic problem analysis including but not limited to applications porting, performance tuning, pre-post processing,

	data access. Higher Level support receives issues that are escalated and routed from First Level Support.
Class:	Core
Provider:	Tier-0 site + WP6 + WP7
Reference:	User Agreement, Contributor Agreement, PRACE-1IP D6.1
Category:	User
Software:	RT-TTS