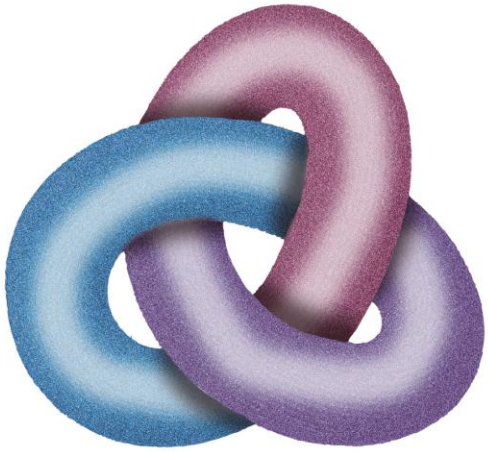

DRIHM

DISTRIBUTED RESEARCH INFRASTRUCTURE FOR HYDRO-METEOROLOGY

D5.4: Report on Support Process Definition

Abstract: This document describes the outcome of an assessment of support processes within the European e-infrastructure setup and a resulting DRIHM (operational) support model.

DRIHM (G.A. n° 283568) is co-Funded by the EC under 7th Framework Programme

DRIHM
DISTRIBUTED RESEARCH INFRASTRUCTURE FOR HYDRO-METEOROLOGY

Document Information Page

Contract Number	283568
Project Name	Distributed Research Infrastructure for Hydro-Meteorology
Project Acronym	DRIHM
Deliverable Number	D5.4
Deliverable Name	Report on Support Processes Definition
Work Package Number	5
Work Package Name	Infrastructure Operation and Management, Data and Resource Management
Deadline	Month 6
Version	2
Dissemination Level	Public
Nature	Report
Lead Beneficiary	LMU

DRIHM
DISTRIBUTED RESEARCH INFRASTRUCTURE FOR HYDRO-METEOROLOGY

Table of Contents

1 Executive Summary

This document is the initial version of deliverable D5.4 of task WP5.3 of the DRIHM work package 5. Deliverable D5.4 serves two purposes:

1. It defines the DRIHM support processes for e-Infrastructure operation. One possibility is to base on the ISO/IEC 20000 standards which are widely used in large-scale IT-infrastructures and find great acceptance;
2. It defines the necessary templates for incident and problem reporting.

The deliverable starts with an overview of the support processes as they are currently implemented in European e-infrastructures with relevance to DRIHM. These are the Partnership for Advanced Computing in Europe (PRACE; and its predecessor the Distributed European Infrastructure for Supercomputing Applications (DEISA)), the European Grid Initiative (EGI) and the National Grid Initiatives (NGI).

DRIHM users (scientists and citizen scientists) need to adhere to the specific infrastructure procedures and policies in order to successfully use the envisioned DRIHM services. While the DRIHM operational model as defined in [6] specifies how to deploy services and how to assure the quality of services, this document specifies the necessary processes to support users (prior to and post mortem of using DRIHM services), administrators and Virtual Organizations (VO).

This report is a living document the initial version of which is due in month 6. Subsequent versions will be published as addenda to this report in months 18, 30, and 42. It should be noticed that the deliverables D5.1 (Report on the Assessment of Operational Procedures and Definition of the DRIHM Operational Model) [6] and D5.4 (Report on Support Process Definition) are closely related.

2 Introduction

One of the main goals of the DRIHM project is the implementation and operation of a distributed and inter-organisational IT-infrastructure for hydro-meteorologic research (HMR) capable of supporting the execution of complex HMR workflows as described in [1]. In order to successfully fulfil the objectives, DRIHM partners need not only to comply with procedures and policies as defined by European e-infrastructures; they also need to be aware of the respective support processes in order to resolve incidents and problems encountered pre-operationally, operationally, and post mortem. Other support processes may follow in the future.

This document consists of two parts:

1. It defines the DRIHM support processes (incident management, problem management, configuration management, etc.);
2. It defines the necessary templates for incident and problem reporting.

3 Starting Points

Before defining the DRIHM support processes we will assess both the *current* environment and the *target* situation. The current environment includes the European e-Infrastructures as such. The target situation relates to the ISO/IEC 20000 specification the aim of which is to provide a common reference standard for all organizations (real ones and virtual ones like DRIHM) that deliver IT services for internal or external clients. ISO/IEC 20000 is strongly related to the IT Infrastructure Library (ITIL), a collection of best practices for service management. ISO/IEC 20000 represents the respective quality benchmark. More information on ISO/IEC 20000 and ITIL can be found in the dedicated literature (for example http://www.bs15000.org.uk/books.htm).

3.1 Summary of an Assessment of European e-Infrastructures

This section briefly summarizes the *operational* procedures for DEISA/PRACE, EGI, and the national Grid initiative (NGI). For further details see [6].

The European distributed computing landscape is dominated by EGI [3] and PRACE [4] / DEISA [2], (see also Figure 1).

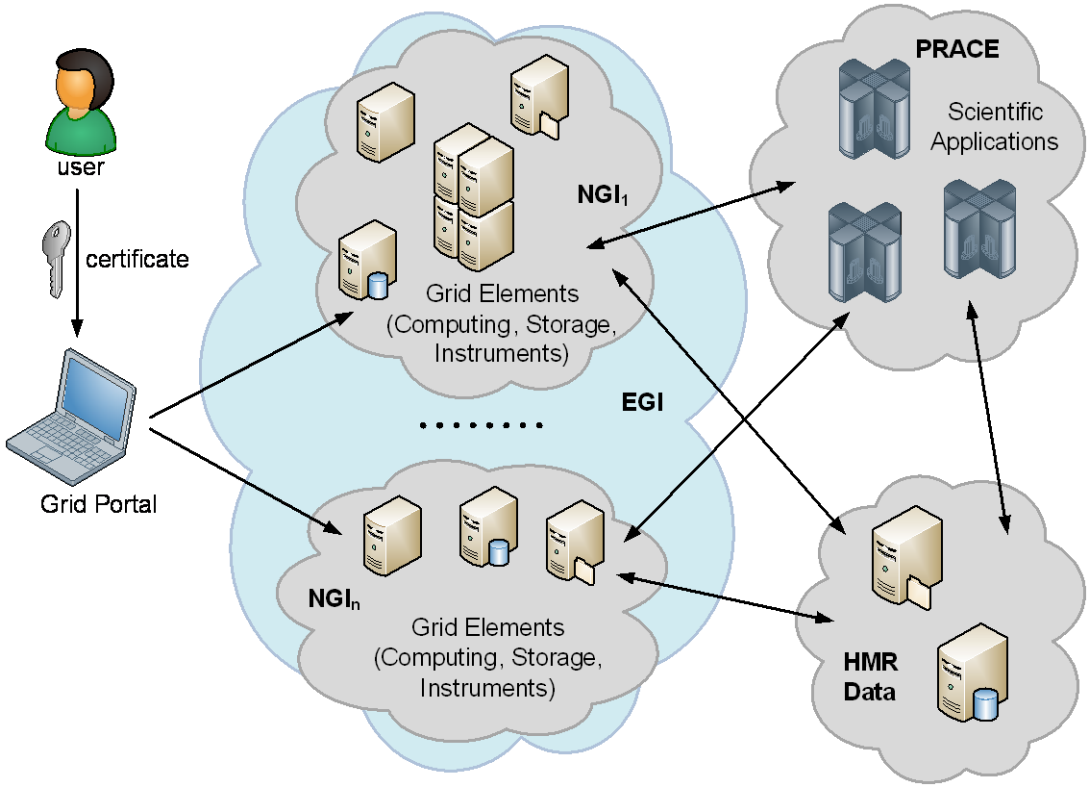

Figure 1: European e-infrastructures in the DRIHM context

The Partnership for Advanced Computing in Europe, PRACE, provides a unique persistent pan-European research infrastructure for HPC with up to six top systems well integrated into the European HPC ecosystem. Each system provides computing power of several Petaflop/s (one quadrillion operations per second) in midterm. Long term PRACE aims at Exaflop/s (one quintillion) computing power. This infrastructure is managed as a single European entity.

The partnership was established through the close collaboration of the European countries that prepared the legal, financial, and technical basis of the project. The First Implementation Phase of PRACE is in line with the objectives of the PRACE Research Infrastructure organisation which can be characterised by coordinated system selection and design, coherent management of the distributed infrastructure, software deployment, porting, scaling, optimising applications and promoting and advancing application development and the skills.

DEISA, the Distributed European Infrastructure for Supercomputing Applications (not shown in Figure 1), is a consortium of leading national supercomputing centres that aims to foster pan-European computational science research. DEISA deploys and operates a persistent, production quality, distributed supercomputing environment with continental scope facilitating the delivery of operational solutions for a European HPC eco-system as suggested by the European Strategy Forum on Research Infrastructures (ESFRI) [5]. By the time of writing this deliverable, the DEISA mission has been completed and services have been handed over to PRACE.

The goal of EGI, the European Grid Initiative, is to enable the provisioning of a sustainable, reliable e-infrastructure to European scientists and their collaborating international partners that supports their needs for large-scale computing and storage systems. For achieving this goal, EGI is collecting user requirements to determine adequate support levels for current and future user communities, as for example specified by the ESFRI projects [5], but also for consortia such as DRIHM and the hydro-meteorological communities. EGI also supports the user communities to migrate their critical services and tools from a centralised support model to one driven by their own individual communities (see below).

While EGI itself is a partnership between the National Grid Initiatives (NGIs) and a coordinating body, the EGI.eu organization, to operate a sustainable, pan-European Grid infrastructure for international scientific communities, the NGIs are national (legal) entities charged with taking care of national Grid infrastructure related to their countries. For a complete list of the EGI European resource infrastructure providers we refer to the information provided on the EGI site https://www.egi.eu/infrastructure/Resource-providers/index.html. The core EGI resource providers fall into one of the following two categories: They either belong to one of the 33 National Grid Initiatives (NGIs), or they belong to one of the European Intergovernmental Research Organisations (EIROs) like the European Organization for Nuclear Research (CERN) or the European Molecular Biology Laboratory (EMBL).

The objective of the National Grid Initiatives is to provide a reliable and secure e-infrastructure by enabling carrier grade Grids and Clouds for academic communities. For example, the German NGI-DE started 2010, the partners, however, have been involved in Grid computing since 1997, mainly in the D-Grid initiative. NGI-DE is under the responsibility of the Gauß-

Allianz (http://www.gauss-allianz.de/?lang=en), a German association in which academic computing centres team up to create the necessary infrastructure for the future of HPC and Grid computing on a national level.

The total number of CPU cores provided by the various NGIs may be derived from Figure 2 [7].

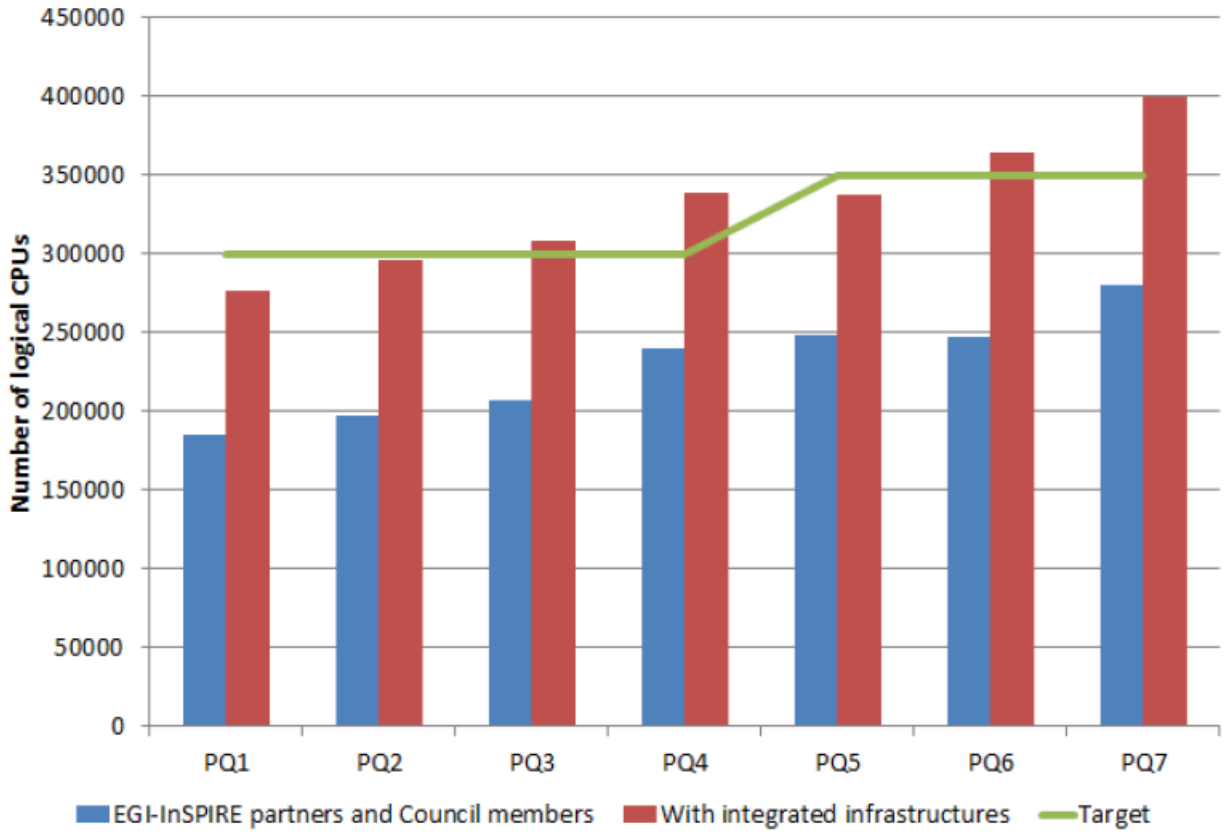

Figure 2: Total number of CPU cores provided by EGI Resource Providers (RP) from June 2010 to January 2012 by RPs who are EGI-InSPIRE partners or EGI Council members (left bar), and the amount of resources contributed together with integrated infrastructures (right bar) [7]

3.2 Summary of an Assessment of the ISO/IEC 20000 Resolution Processes

The ISO/IEC 20000 standards are widely used and find great acceptance in the operation and management of large-scale IT-infrastructures. The ISO/IEC 20000 resolution processes cover both the incident and problem management processes. Although intertwined, these processes have to be considered standalone. While incident management deals with the recovery of the service for the user, problem management deals with the identification and elimination of root causes in the case of service disruptions and therefore tried to ensure a resilient and robust service infrastructure.

The objective of incident management processes is to recover the agreed service and to ensure service enquiries are fulfilled as reliable as possible. However, the processes must focus on the restoration of the IT services per se and *not* on the identification of the root causes. Incident management thus comprises receiving calls, recording, prioritization, taking care of security provisions as well as following up on the incident processing status. It should also govern the agreements on fault processing with the user as well as any escalation procedures. All incidents must be recorded in such a way as to enable the relevant information to rectify error events. The progress of work is assumed to be reported to the current and any potential personnel affected. All activities must be fully recorded in incident tickets. Wherever possible, users must be able to continue their work in an appropriate way – even if workarounds have to be applied.

The objective of problem management on the other hand is to minimize the disruption to and the impact on the user's work by proactively identifying and analyzing the root causes of service incidents and by managing problems until these are rectified and re-occurrence is excluded. Problems are to be classified as known errors as soon as the root cause of the incident is known and a solution method for avoiding such incidents has been found. For incident management to receive an optimum supply of information, all known errors and IT services affected must be documented and the associated configuration items identified. Known errors should only be closed once a definitive, successful solution has been found. Once the root cause has been identified and a decision has been reached on the solution, this

solution must be dealt with by appropriate change management processes. Information on the progress, potential workarounds or permanent solutions must be made available to all parties involved.

The closure of problem tickets should always be carried out in accordance with the following reviews:

- Has the solution been precisely documented?
- Has the root cause been categorized in order to provide support for future further analyses?
- Have the users and support employees effected been informed of the solution?
- Has the user confirmed that he/she accepts the solution?
- Has the user been informed if no solution has been found?

Setting priorities in dealing with disruptions and problems is based on the two criteria of *impact* (negative effect on the service) and *urgency* (urgency as a result of the current situation). The impact should be based on the extent of the interruption to user work whilst the urgency is based on the timescale between the incident occurring and its negative impact on the service's availability or reliability.

4 Current Support Concepts of European e-Infrastructures

The support concepts of the various European e-Infrastructures differ slightly.

4.1 PRACE Support

The PRACE support is generally described in the PRACE Best Practices (http://www.prace-project.eu/Best-Practice-Guides?lang=en) which, however, differ between the various PRACE sites. Typically, PRACE service desks accept tickets as the one in Figure 3:

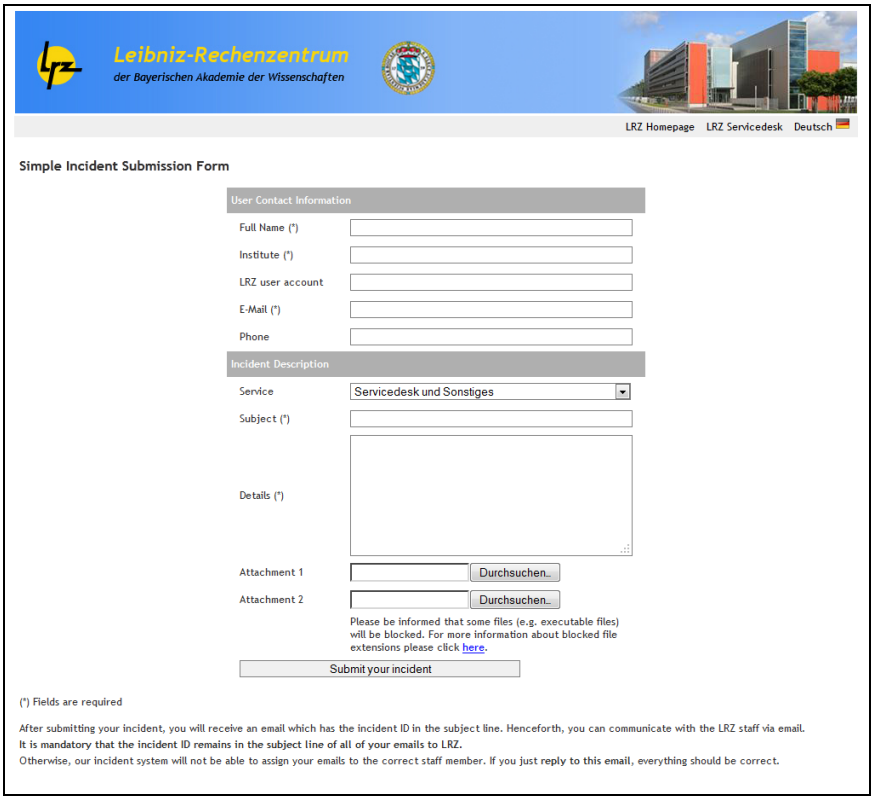

Figure 3: Example of creating a PRACE ticket

While these processes are mainly site-specific, PRACE also operates a dedicated Helpdesk as the first point of contact for all users whenever they have any issues with or questions about PRACE services and facilities. The Helpdesk functionality is accessed through a web interface at https://tts.prace-ri.eu/SelfService/. For more information on the PRACE Helpdesk Guide we refer to http://www.prace-project.eu/Helpdesk-Guide,264?lang=en. The Helpdesk is based on Best Practical's public domain Request Tracker RT (http://bestpractical.com/rt/) which itself facilitates ISO 20000 compliance. Figure 4 depicts an example of the PRACE Helpdesk open ticket view.

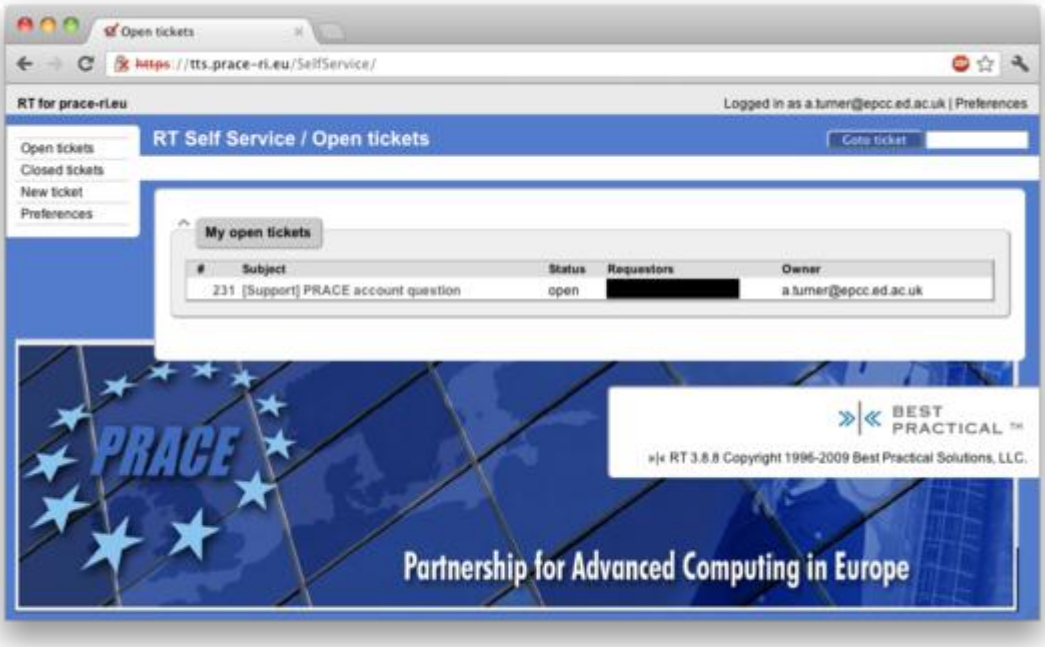

Figure 4: Example of a PRACE Helpdesk Open Ticket view (Source: http://www.prace-project.eu/Helpdesk-Guide,264?lang=en)

4.1.1 DEISA Support

Following http://www.deisa.eu/usersupport/primer/access-to-the-user-support, the DEISA User Support comprises two stages: a preparation stage and a production stage. In the preparatory phase of a project the support questions will typically be related to obtaining certificates and accounts and to the user's applications, e.g., concerning the optimization strategy, the porting of code to the different HPC platforms in DEISA or the choice of the DEISA middleware. These will be addressed by the Application Support team at the project Home Site. The Home Site is assigned to the user when a project is accepted.

The production stage begins once the infrastructure is in place to provide an efficient runtime environment and when the execution site has allocated resources to the project. Typical questions in this stage are about availability of resources, functioning of batch systems or the Common Production Environment etc.

During both stages, all questions arising must be addressed to the central DEISA Helpdesk by either reporting the problem directly into the DEISA Trouble Ticket System via the Web interface or by sending an e-mail describing the problem to the DEISA Helpdesk. A typical example of a DEISA ticket is given in Figure 5

It should be noticed that the DEISA Helpdesk/ticketing system does not comply to the ISO/IEC 20000 standard.

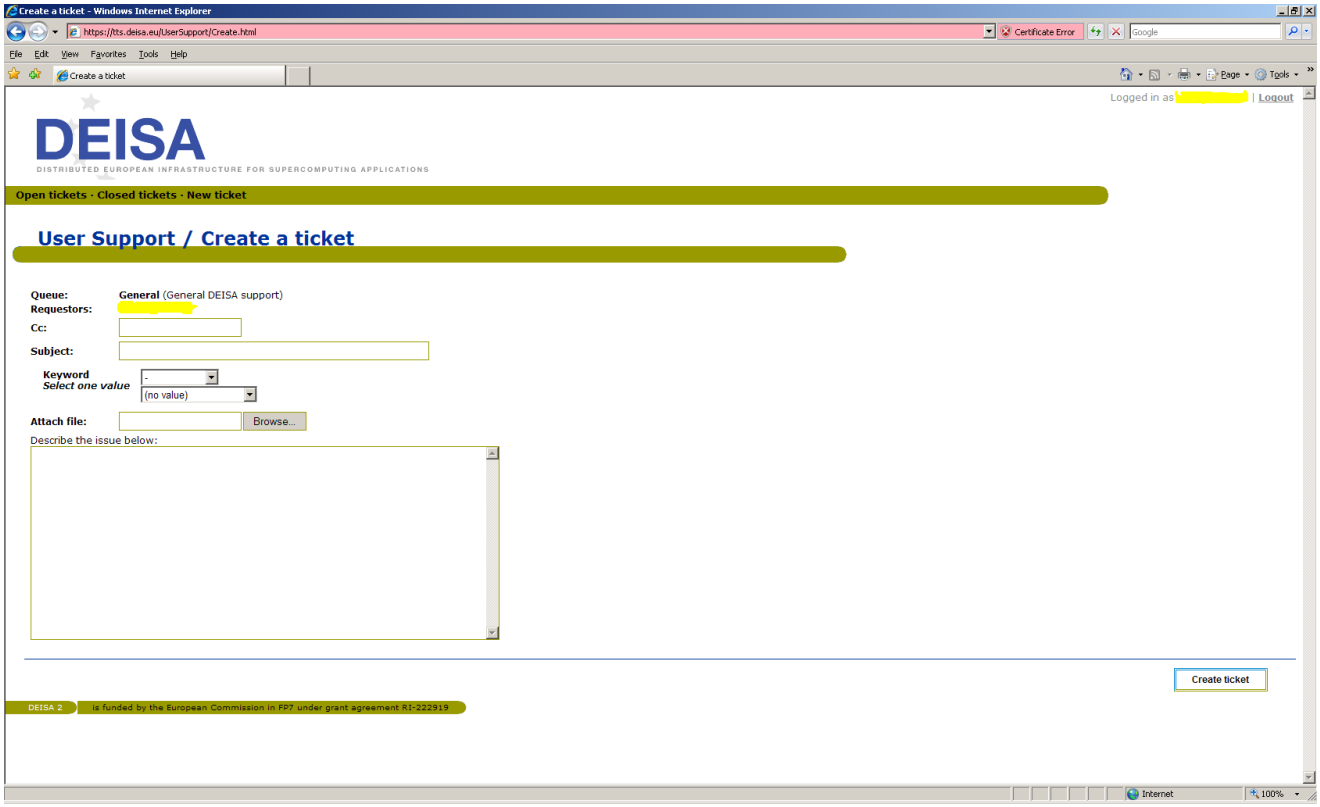

Figure 5: Creation of a DEISA ticket (Source: http://www.deisa.eu/usersupport/primer/access-to-the-user-support)

4.2 EGI Support

The EGI support is described in detail at https://www.egi.eu/how-do-I/report_an_issue.html and https://www.egi.eu/how-do-I/get_support.html and all linked pages.

A typical example of the EGI incident response procedure is given in [8]. It is depicted in Figure 6.

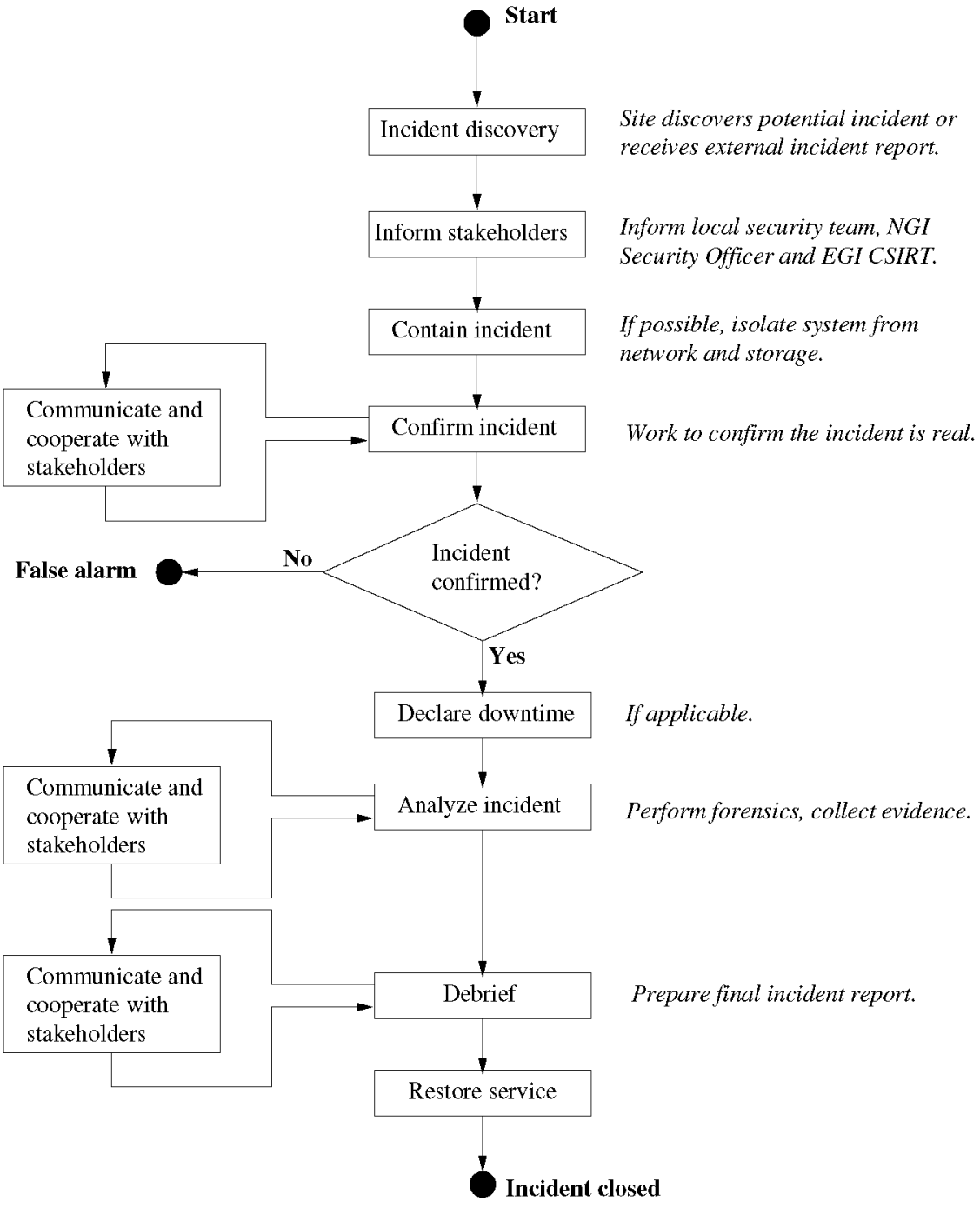

Figure 6: Flow Chart for Incident Response in EGI [8]

The central contact point for users of the European Grid Infrastructure needing to report a problem, to issue a service request or to report a requirement for the technology in use is the EGI Helpdesk. The EGI Helpdesk is also used as the central incident management tool for EGI. For privacy and security reasons most parts of this website can only be accessed with a valid Grid certificate or after a successful registration. The EGI Helpdesk is accessed through the Global Grid User Support (GGUS, https://ggus.eu/pages/home.php) system as the primary means by which users request support when they are using the Grid. The GGUS system creates a trouble ticket to record the request and tracks the ticket from its creation through to its solution. The user of the system should not need to know any of the details of what happens to the ticket in order to get it from creation to solution. The information required for submitting a GGUS ticket is given in Figure 7.

The EGI GGUS Helpdesk is also based on Best Practical's public domain Request Tracker RT (http://bestpractical.com/rt/) which itself facilitates ISO 20000 compliance.

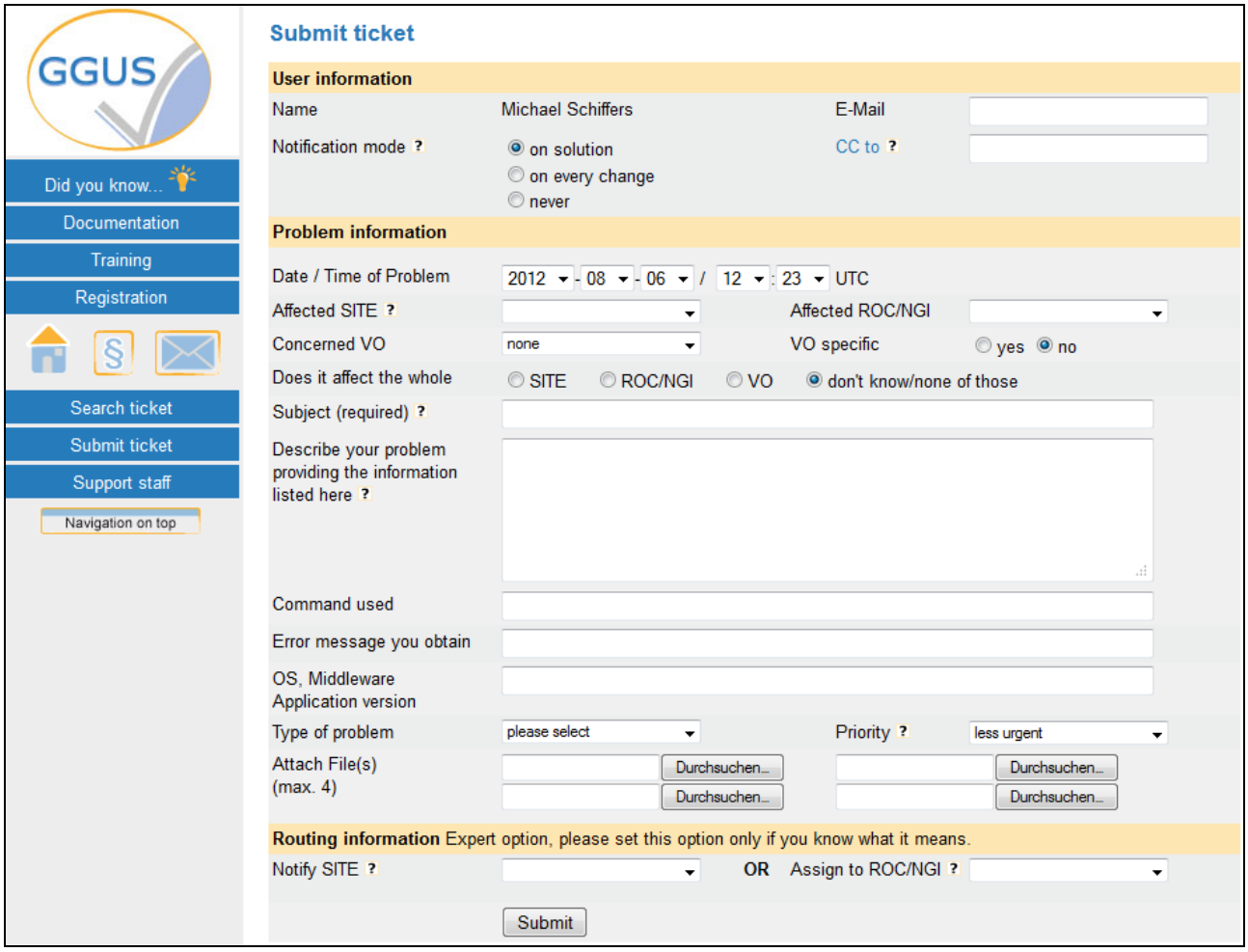

Figure 7: Creating an EGI GGUS ticket

4.3 NGI Support

The National Grid Initiatives have implemented individual support structures and processes using various systems. The German national Grid, NGI-DE, for example, uses an RT-based ticketing system (see Figure 8)

Figure 8: German NGI ticketing

Other NGIs base their incident and problem management more or less on the LCG/EGEE Incident Handling and Response Guide. Please note, however, that this guide is not ISO/IEC 20000 compliant. Examples are the Dutch BigGrid (http://www.biggrid.nl/fileadmin/documents/policies/Incident_Response_Guide.pdf) and the Baltic Grid (http://www.balticgrid.org/Deliverables/pdfs/BGII-DSA2-5-v1-2-IMCSUL-IHRPolicy.pdf). Again others (for example France, Italy) are mainly based on email-ticketing.

5 Key Points of a DRIHM Support Concept

For sustainability reasons, the DRIHM support concept needs to cover several categories to be handled uniformly in a standardised way (ISO/IEC 20000 compliance) through an open source ticketing system. These categories cover at least

1. Usage support
2. Administrative support
3. Post-mortem support

In this report (the first of a series of reports) we focus on the key points only. Subsequent versions will go into further details.

5.1.1 Usage Support

DRIHM users (scientists and citizen scientists) will receive support on how to use the DRIHM services. For this purpose DRIHM provides

- How-to manuals on the DRIHM web sites with descriptions of how to deploy and how to use the DRIHM services
- Education classes and corresponding training material during the DRIHM seasonal schools
- Developer contacts
- DRIHM User Forum (DUF)

The material will focus on achieving two goals: First, it will provide detailed information and guidance to DRIHM users who want to run complex workflows; second, it will act as a reference for e-infrastructure administrators charged with the installation and configuration of DRIHM services on production e-infrastructures. The material will be updated regularly and it will play an important role in achieving the sustainability goals of the DRIHM project.

Introductory lectures and training course will be provided as a part of the DRIHM dissemination activities led by WP2 and supported by all project partners. The main focus of these activities

will be to inform user communities about DRIHM services and help them in the initial usage of scientific workflows based on DRIHM service.

5.1.2 Administrative Support

DRIHM will not only provide administrative support for installation, configuration and maintenance of deployed services, but also for setting up, maintaining and termination of VOs on European Grid infrastructures. It includes such tasks as authentication, authorization, certificate management, accounting and billing.

DRIHM will support two classes of VOs: one for users interested in testing and experimentation and another one for communities wishing to use the DRIHM services in fulfilling their own research activities. WP6 will provide support to both classes. Comprehensive documentation, including but not limited to installation and administration manuals, user guides, tutorials and sample videos, will be offered for all DRIHM services.

Following [6], prior to the deployment into the DRIHM e-infrastructure[1], all software components will pass a rigorous validation and testing process as defined by WP6. The tests have to confirm that the software to be deployed fulfills the functional requirements defined by the developers and that it is able to interact with the environment, for instance the operating system, drivers and low level libraries and applications, without disturbing production systems in any undesired way. During the later stages of the project the DRIHM services will also be tested to ensure their interoperability with each other. To support the software validation process a specific DRIHM test bed environment will be created to act as a platform for testing activities and experimentation with the DRIHM software components, for instance the scientific applications developed by WP7 and WP8. Production quality resources for the test bed will be provided by all partners upon request. A detailed description of the test bed will be available in February 2013.

[1] By DRIHM e-infrastructure we understand an existing e-infrastructure augmented by specific DRIHM services.

All successfully validated software components will be passed to WP6 for deployment on the DRIHM e-infrastructure. Each component will be assigned a WP6 service expert responsible for coordinating its installation, configuration and maintenance. To facilitate the deployment process WP6 develops a DRIHM Service Description Form. The form is used to describe the software components including their essential characteristics like system and security requirements. It is expected that the form will be filled out for each of the components to be deployed and provided to the responsible application expert who will use the information during the initial installation phase.

All deployed DRIHM components will be monitored to ensure their availability and correct functionality. Monitoring will be performed using applications and tools selected by the DRIHM Steering Committee according to functional requirements determined by WP7 and WP8. During the selection process DRIHM will pay special attention to the monitoring solutions used by DEISA/PRACE and EGI/NGI to guarantee compatibility with European e-infrastructures in this area.

Monitoring results will be used by other work packages either to extend the service functionality and improve the service quality by deploying additional monitoring solutions (WP6), or to report on the availability (WP2).

Detected incidents and unexpected behavior of the DRIHM services will be directly reported to WP6 via the DRIHM Ticketing System [6]. Each incident will be classified based on its impact on the DRIHM e-infrastructure and assigned to the service expert responsible for the failing component. The experts will analyse and attempt to resolve the problem. If successful, all parties affected by the problem will be informed and the solution will be documented in the DRIHM knowledge base. In situations when members of WP6 cannot resolve a problem, other work packages will be asked for assistance. If necessary, the problem will be escalated to the developers of the respective component (which may have been developed externally).

All monitoring data collected by DRIHM will be archived and used for reporting and quality assurance. General information about availability and functionality of DRIHM services will be published on the DRIHM web site and used for dissemination and reporting. The production status of the DRIHM services will be regularly evaluated by the project partners, in particular

by the DRIHM Steering Committee. The committee will closely observe the service quality levels and the overall availability of the DRIHM e-infrastructure and will issue recommendations if the values fall below defined levels.

5.1.3 Post Mortem Support

Post mortem support will start with the operation of the DRIHM baseline version of experiment suite 1 and will be provided in a number of ways, including ticketing systems, phone support and email support.

DRIHM will operate a help desk and provide VOs and user communities with comprehensive technical support. Reported problems will be handled by WP4 and WP6 in close co-operation with all other work packages according to the DRIHM support procedures. Issues beyond the expertise of DRIHM will be escalated to external entities, such as application developers or service providers.

5.1.4 Implementation

In order to be flexible enough while at the same time adhering to standards like ISO/IEC 20000, DRIHM will implement an all-comprehensive DRIHM ticketing system based on the public domain Request Tracker (RT). Due to its ISO/IEC 20000 compliance the DRIHM-RT will achieve most of the objectives for incident and problem handling for usage support, administrative support, and post-mortem management. The RT page http://bestpractical.com/rt/screenshots.html contains screenshots which may give an idea of how to use RT.

A first DRIHM RT will be available in February 2013.

6 Conclusion

This document is the first version of deliverable D5.4 of task WP5.1 of the DRIHM work package 5. It assesses the major support concepts used across the European e-infrastructures related to the DRIHM project and it defines the key points of an ISO/IEC 20000 DRIHM support concept.

The considered e-infrastructures are PRACE (and its predecessor DEISA), EGI and the national Grid initiatives. The relation between these infrastructures and their specifics are described before reviewing the basics of the ISO/IEC 20000 resolution processes (incident management, problem management).

Starting from the procedures inherent to these infrastructures, the DRIHM support concept describes the mechanisms for supporting users and Virtual Organizations (VO).

7 Acronyms and References

7.1 Acronyms

DEISA	Distributed European Infrastructure for Supercomputing Applications
EGI	European Grid Initiative
ESFRI	European Strategy Forum on Research Infrastructures
HMR	Hydro-Meteorologic Research
HPC	High Performance Computing
NGI	National Grid Initiative
PRACE	Partnership for Advanced Computing in Europe
VO	Virtual Organisation

7.2 References

[1] DRIHM Description of Work, Part B

[2] DEISA: http://www.deisa.eu/

[3] EGI: http://www.egi.eu/

[4] PRACE: http://www.prace-project.eu/

[5] ESFRI: http://ec.europa.eu/research/esfri/

[6] DRIHM Deliverable D5.1: *Report on the Assessment of Operational Procedures and Definition of the DRIHM Operational Model*, 2012

[7] EGI-InSpire: Annual Report on the EGI Production Infrastructure, EU Deliverable D4.5, 2012, https://documents.egi.eu/public/RetrieveFile?docid=1059&version=9&filename=EGI-D4.5-final.pdf

[8] EGI.eu: Security Incident Response Procedure, 2011, https://documents.egi.eu/public/RetrieveFile?docid=710&version=3&filename=EGI-Procedure-CSIRT-710-V3%20.pdf